Generating Prime Numbers

Lauren Snyder

1 Historical Background

A number p is prime if it is a natural number greater than 1 whose only divisors are 1 and p. The first 25 prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97. They are quite randomly distributed among the natural numbers with no natural way of getting from one prime number to the next prime number. Each number must be tested for primality individually. This has intrigued many mathematicians since antiquity and has directed their attention to the set of primes. They have attempted to find a formula to reliably generate and describe the primes. It may not be clear what the phrase "find a formula" means. Ribenboim [4] provides three possible definitions:

(a) Find a function f such that $f(n)$ is the nth prime p_n.

(b) Find a function f such that $f(n)$ is always prime, and if $n \neq m$ then $f(n) \neq f(m)$.

(c) Describe the set of prime numbers by means of polynomials.

According to [4], condition (a) requires that all primes must be found in correct order and known functions in this category are generally infeasible to compute in practice. For example, Gandhi's formula [4] is

$$p_n = \left\lfloor 1 - \log_2 \left(-\frac{1}{2} + \sum_{d|P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right\rfloor$$

where $P_n = p_1 p_2 \cdots p_n$, and μ is the Mobius function,

$$\mu(p_1^{a_1} \cdots p_k^{a_k}) = \begin{cases} (-1)^k, & \text{if } a_1 = \cdots = a_k = 1 \\ 0, & \text{otherwise.} \end{cases}$$

Another formula is Willans' Formula [4]

$$p_n = 1 + \sum_{i=1}^{2^n} \left\lfloor \left(\frac{n}{\sum_{j=1}^{i} \left\lfloor \left(\cos \frac{(j-1)!+1}{x} \pi \right)^2 \right\rfloor} \right)^{1/n} \right\rfloor .$$

Both are essentially versions of the sieve of Eratosthenes, which provides an algorithm to get the prime numbers up to a certain limit. The algorithm is described in [2] as follows:

Given n, the prime numbers up to n are identified.

(1) Let n be a positive integer; set $S = \{2, 3, \cdots, n\}$.

(2) For $2 \leq i \leq \lfloor \sqrt{n} \rfloor$, do:
If i has not been crossed out in S, then cross out all proper multiples of i in S.

(3) The elements of S that are not crossed out are the prime numbers up to n.

Also, Gandhi's formula depends on the Möbius function $\mu(d)$, and Willans' formula comes from Wilson's theorem. From [2], Wilson's theorem is stated as follows.

Theorem 1. *The congruence*

$$(n-1)! \equiv -1 \mod n$$

holds if and only if n is prime.

In [4], Ribenboim states that in order to satisfy condition (b) we must find a way to generate infinitely many different primes. The primes do not necessarily need to be in proper order and the list need not be all inclusive. An example from [5] is the function provided by Mills, who proved that there exists a real number A such that $\lfloor A^{3^n} \rfloor$ is prime for $n \geq 1$. An approximation to a suitable A is found by working backward from known large primes.

n	$n^2 - n + 11$
1	11
2	13
3	17
4	23
5	31
6	41
7	53
8	67
9	83
10	101

Table 1: The primes generated by $p(n) = n^2 - n + 11$

We turn to condition (c) to attempt to describe the prime numbers. Is there a polynomial that always returns a prime number when positive whole numbers are substituted for the unknowns? A possible example is Euler's polynomial $n^2 - n + 41$ of 1772 which is prime for $1 \leq n \leq 40$. However, when $n = 41$, we have $n^2 - n + 41 = 41^2 - 41 + 41 = 41^2$, a composite number. Another example is $p(n) = n^2 - n + 11$. Table 1 shows the primes generated by $p(n)$. Notice when $n = 11$, we have $11^2 - 11 + 11 = 11^2$, a composite number.

Consider the "Prime Spiral", beginning with $p = 11$ at the center.

111	110	109	108	107	106	105	104	103	102	**101**
112	75	74	73	72	71	70	69	68	**67**	100
113	76	47	46	45	44	43	42	**41**	66	99
114	77	48	27	26	25	24	**23**	40	65	98
115	78	49	28	15	14	**13**	22	39	64	97
116	79	50	29	16	**11**	12	21	38	63	96
117	80	51	30	**17**	18	19	20	37	62	95
118	81	52	**31**	32	33	34	35	36	61	94
119	82	**53**	54	55	56	57	58	59	60	93
120	**83**	84	85	86	87	88	89	90	91	92
121	122	123	124	125	126	127	128	129	130	131

Notice that the numbers produced by $p(n)$ fall along the diagonal from the top right corner down to the bottom left, excluding 121. [3]

There have been several polynomials discovered since Euler's to generate primes up to a limit. In [3], Pegg gives examples $36x^2-810x+2753$ with 45 distinct primes, $x^4 - 97x^3 + 3294x^2 - 45458x + 213589$ with 49 distinct primes, and $(x^5 - 133x^4 + 6729x^3 - 158379x^2 + 1720294x - 6823316)/4$ with 57 distinct primes. Those examples give more primes, but for polynomials in one unknown it can be shown that it is not possible to always return a prime number. In [1] it is stated that a nonconstant polynomial $f(x)$ with integer coefficients produces at least one composite image. In [1] they improve the result by proving the following theorem.

Theorem 2. *Given a positive integer n, $f(x)$ takes an infinite number of values that are divisible by at least n distinct primes, and an infinite number of values that are divisible by p^n for some prime p.*

In [4] the theorem is stated as follows:

Theorem 3. *If $f(x)$ is a polynomial with integer coefficients of degree $d \geq 1$, whose highest degree term has a coefficient greater than or equal to 1, then there are infinitely many $n \geq 1$ such that $f(n)$ is a composite number.*

These theorems explain why mathematicians have been unsuccessful in finding a formula of this form. We revise the question: Is there a naturally occurring function that always generates primes?

2 A New Prime-Generating Recurrence

Eric Rowland [5] discussed a recursively defined function discovered in 2003 at the NKS Summer School. The recurrence produces a prime at each step, but as required by condition (b), the primes are not distinct nor all inclusive. The sequence a_n was defined as follows: Let $a_1 = 7$ and

$$a_n = a_{n-1} + \gcd(n, a_{n-1}) \text{ for } n > 1. \tag{1}$$

The first few terms of the sequence $\{a_n\}$ are

$$7, 8, 9, 10, 15, 18, 19, 20, 21, 22, 33, 36, 37, 38, 39, 40, 41, 42, 43, 44, \ldots$$

Let $g_n = a_n - a_{n-1} = \gcd(n, a_{n-1})$ for $n \geq 2$. Then g_n is

$$1, 1, 1, 5, 3, 1, 1, 1, 1, 11, 3, 1, 1, 1, \ldots$$

In [5] the following terms of g_n were listed:

1, 1, 1, 5, 3, 1, 1, 1, 1, 11, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 23, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 47, 3, 1, 5, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 101, 3, 1, 1, 7, 1, 1, 1, 1, 11, 3, 1, 1, 1, 1, 1, 13, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 233, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 467, 3, 1, 5, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, . . .

Notice that this difference sequence appears to be composed entirely of 1's and primes. Discarding the ones we are left with the following sequence of primes as provided in [5].

5, 3, 11, 3, 23, 3, 47, 3, 5, 3, 101, 3, 7, 11, 3, 13, 233, 3, 467, 3, 5, 3, 941, 3, 7, 1889, 3, 3779, 3, 7559, 3, 13, 15131, 3, 53, 3, 7, 30323, 3, 60647, 3, 5, 3, 101, 3, 121403, 3, 242807, 3, 5, 3, 19, 7, 5, 3, 47, 3, 37, 5, 3, 17, 3, 199, 53, 3, 29, 3, 486041, 3, 7, 421, 23, 3, 972533, 3, 577, 7, 1945649, 3, 163, 7, 3891467, 3, 5, 3, 127, 443, 3, 31, 7783541, 3, 7, 15567089, 3, 19, 29, 3, 5323, 7, 5, 3, 31139561, 3, 41, 3, 5, 3, 62279171, 3, 7, 83, 3, 19, 29, 3, 1103, 3, 5, 3, 13, 7, 124559609, 3, 107, 3, 911, 3, 249120239, 3, 11, 3, 7, 61, 37, 179, 3, 31, 19051, 7, 3793, 23, 3, 5, 3, 6257, 3, 43, 11, 3, 13, 5, 3, 739, 37, 5, 3, 498270791, 3, 19, 11, 3, 41, 3, 5, 3, 996541661, 3, 7, 37, 5, 3, 67, 1993083437, 3, 5, 3, 83, 3, 5, 3, 73, 157, 7, 5, 3, 13, 3986167223, 3, 7, 73, 5, 3, 7, 37, 7, 11, 3, 13, 17, 3, . . .

It is not clear why g_n should never be composite, but we will provide details of the proof given in [5]. For small initial conditions, it will be shown that the sequence $\{g_n\}$ is always 1 or prime.

3 Observations

Rowland [5] describes the intial observations made that led to the discovery of the proof that the sequence $\{g_n\}$ is always 1 or prime. Table 2 was given in [5] and summarizes the first few terms of a_n and g_n as well as other quantities $\Delta_n = a_{n-1} - n$ and a_n/n.

There were four key observations that Rowland listed in [5]. The first observation was that g_n contains long runs of consecutive 1's. Notice that for a given natural number n_1 and $n > n_1$,

$$\begin{aligned} a_{n_1} + \sum_{i=1}^{n-n_1} g_{n_1+i} &= a_{n_1} + g_{n_1+1} + g_{n_1+2} + \cdots + g_{n_1+n-n_1} \\ &= a_{n_1} + g_{n_1+1} + g_{n_1+2} + \cdots + g_n \\ &= a_{n_1} + (a_{n_1+1} - a_{n_1}) + (a_{n_1+2} - a_{n_1+1}) + \cdots + (a_n - a_{n-1}) \\ &= a_n \end{aligned}$$

So if $g_n = 1$ for $n_1 < n < n_1 + k$, then

$$a_n = a_{n_1} + \sum_{i=1}^{n-n_1} g_{n_1+i} = a_{n_1} + (n - n_1). \tag{2}$$

This means that the difference $a_{n-1} - n = a_n - g_n - n = a_{n_1} - n_1 - 1$, or Δ_n, remains constant in this range.

The second observation Rowland made in [5] was that when the next nontrivial gcd does occur, it appears to divide

$$\Delta_n := a_{n-1} - n = a_{n_1} - 1 - n_1.$$

In Table 2, we notice $5 \mid 5$, $3 \mid 9$, $11 \mid 11$, $3 \mid 21$, $23 \mid 23$, $3 \mid 45$, $47 \mid 47$, etc. We will prove this observation later.

n	Δ_n	g_n	a_n	a_n/n
1			7	7
2	5	1	8	4
3	5	1	9	3
4	5	1	10	2.5
5	5	5	15	3
6	9	3	18	3
7	11	1	19	2.71429
8	11	1	20	2.5
9	11	1	21	2.33333
10	11	1	22	2.2
11	11	11	33	3
12	21	3	36	3
13	23	1	37	2.84615
14	23	1	38	2.71429
15	23	1	39	2.6
16	23	1	40	2.5
17	23	1	41	2.41176
18	23	1	42	2.33333
19	23	1	43	2.26316
20	23	1	44	2.2
21	23	1	45	2.14286
22	23	1	46	2.09091
23	23	23	69	3
24	45	3	72	3
25	47	1	73	2.92
26	47	1	74	2.84615
27	47	1	75	2.77778
28	47	1	76	2.71429
29	47	1	77	2.65517
30	47	1	78	2.6
31	47	1	79	2.54839
32	47	1	80	2.5
33	47	1	81	2.45455
34	47	1	82	2.41176
35	47	1	83	2.37143
36	47	1	84	2.33333
37	47	1	85	2.2973
38	47	1	86	2.26316
39	47	1	87	2.23077
40	47	1	88	2.2
41	47	1	89	2.17073
42	47	1	90	2.14286
43	47	1	91	2.11628
44	47	1	92	2.09091
45	47	1	93	2.06667
46	47	1	94	2.04348
47	47	47	141	3
48	93	3	144	3
49	95	1	145	2.95918
50	95	5	150	3
51	99	3	153	3
52	101	1	154	2.96154
53	101	1	155	2.92453
54	101	1	156	2.88889
⋮	⋮	⋮	⋮	⋮
99	101	1	201	2.0303
100	101	1	202	2.02
101	101	101	303	3
102	201	3	306	3
103	203	1	307	2.98058
104	203	1	308	2.96154
105	203	7	315	3
106	209	1	316	2.98113

Table 2: The first few terms for $a_1 = 7$.

j	n_j	g_n
1	5	5
2	6	3
3	11	11
4	12	3
5	23	23
6	24	3
7	47	47
8	48	3
9	50	5
10	51	3
11	101	101
12	102	3
13	105	7

Table 3: First few values of n for which $g_n \neq 1$.

The most important observation for the proof of the lemma comes about from restricting our attention to the times when the gcd is non-trivial. We notice that $a_n = 3n$ whenever $g_n \neq 1$ which suggests that a_n/n may be worth our attention.

The final observation can be made by making a table of values of n for which $g_n \neq 1$. We let $n_j = j^{\text{th}}$ value of n for which $g_n \neq 1$. In Table 2, we notice regular clusters which indicates a local structure in the sequence as stated in [5]. In a cluster, the first number corresponds to a prime g_n which is relatively large and ends with a relatively small prime. Rowland observes that the ratio between the index n beginning one cluster and the index ending the previous cluster is very nearly 2. For example,

$$11/6 = 1.833333 \qquad 47/24 = 1.958333$$
$$23/12 = 1.816667 \qquad 101/51 = 1.980392$$

4 A Proof that the sequence generates primes

Rowland then established the observations in [5], and we are going to give his proof in this section, making the details more clear. We can

also broaden the result from $a_n/n = 3$ to include when $a_n/n = 2$ for other initial conditions. The following lemma from [5], is instrumental in the proof that the recurrence generates primes, and it proves our observations. The lemma is a generalization, but the calculation in (2) still holds. It allows for the elimination of the intervening runs of 1's.

Lemma 1. *Let $r \in \{2, 3\}$ and $n_1 \geq \frac{3}{r-1}$. Let $a_{n_1} = rn_1$, and for $n > n_1$ let*

$$a_n = a_{n-1} + \gcd(n, a_{n-1})$$

and $g_n = a_n - a_{n-1}$. Let n_2 be the smallest integer greater than n_1 such that $g_{n_2} \neq 1$. Let p be the smallest prime divisor of

$$\Delta_{n_1+1} = a_{n_1} - (n_1 + 1) = (r-1)n_1 - 1.$$

Then

(a) $n_2 = n_1 + \frac{p-1}{r-1}$,

(b) $g_{n_2} = p$, *and*

(c) $a_{n_2} = rn_2$.

Proof. Let $k = n_2 - n_1$. We show that $k = \frac{p-1}{r-1}$. First we need to show $\frac{p-1}{r-1}$ is an integer. Clearly $\frac{p-1}{r-1}$ is an integer if $r = 2$. If $r = 3$, then $(r-1)n_1 - 1$ is odd. This means p is an odd prime, so $\frac{p-1}{r-1}$ is an integer in this case as well.

Now, for $1 \leq i \leq k$ we have

$$\begin{aligned} g_{n_1+i} &= \gcd(n_1 + i, a_{n_1+i-1}) && \text{by definition} \\ &= \gcd(n_1 + i, a_{n_1} + (n_1 + i - 1 - n_1)) && \text{by (2)} \\ &= \gcd(n_1 + i, a_{n_1} + i - 1) \\ &= \gcd(n_1 + i, rn_1 + i - 1). \end{aligned}$$

Therefore, g_{n_1+i} divides both $n_1 + i$ and $rn_1 + i - 1$. So g_{n_1+i} divides both their difference

$$(rn_1 + i - 1) - (n_1 + i) = (r-1)n_1 - 1$$

and their linear combination

$$r \cdot (n_1 + i) - (rn_1 + i - 1) = (r-1)i + 1. \tag{3}$$

Show $k = \frac{p-1}{r-1}$ by showing $k \leq \frac{p-1}{r-1}$ and $k \geq \frac{p-1}{r-1}$. First, show $k \geq \frac{p-1}{r-1}$. We know g_{n_1+k} divides $(r-1)n_1 - 1$ and by our assumption $g_{n_2} = g_{n_1+k} \neq 1$, $g_{n_1+k} \geq p$. Since g_{n_1+k} also divides $(r-1)k+1$, we have

$$p \leq g_{n_1+k} \leq (r-1)k + 1$$

So $k \geq \frac{p-1}{r-1}$.

Next, we show $k \leq \frac{p-1}{r-1}$. We have $g_{n_1+i} = 1$ for $1 \leq i < \frac{p-1}{r-1}$, and we show that $i = \frac{p-1}{r-1}$ produces a nontrivial gcd. We have

$$\begin{aligned}
g_{n_1+\frac{p-1}{r-1}} &= \gcd\left(n_1 + \frac{p-1}{r-1}, rn_1 - 1 + \frac{p-1}{r-1}\right) \\
&= \gcd\left(\frac{(r-1)n_1 + p - 1}{r-1}, \frac{(rn_1-1)(r-1) + p - 1}{r-1}\right) \\
&= \gcd\left(\frac{((r-1)n_1 - 1) + p}{r-1}, \frac{r(rn_1-1) - rn_1 + 1 + p - 1}{r-1}\right) \\
&= \gcd\left(\frac{((r-1)n_1 - 1) + p}{r-1}, \frac{r \cdot (rn_1 - 1 - n_1) + p}{r-1}\right) \\
&= \gcd\left(\frac{((r-1)n_1 - 1) + p}{r-1}, \frac{r \cdot ((r-1)n_1 - 1) + p}{r-1}\right)
\end{aligned}$$

By definition of p, $p \mid ((r-1)n_1 - 1)$ and $p \nmid (r-1)$. We can conclude this since $r - 1 = 1$ or 2 and p is odd. Thus p divides both arguments of the gcd, so $g_{n_1+\frac{p-1}{r-1}} \geq p$. Therefore $k = \frac{p-1}{r-1}$, and we have shown (a).

Now we will show $g_{n_2} = p$. Since $n_2 = n_1 + k = n_1 + \frac{p-1}{r-1}$, we have $g_{n_1+\frac{p-1}{r-1}}$ divides $(r-1)\frac{p-1}{r-1}+1$ by (3), using $\frac{p-1}{r-1}$ for i. Thus $g_{n_2} = g_{n_1+\frac{p-1}{r-1}}$ divides $(r-1)\frac{p-1}{r-1} + 1 = p$. Since p is prime and $g_{n_2} \neq 1, g_{n_2} = p$. Therefore, this proves (b).

We now have $g_{n_2} = p = (r-1)k + 1$, so to obtain (c) we compute

$$\begin{aligned}
a_{n_2} &= a_{n_2-1} + g_{n_2} \\
&= a_{n_1+k-1} + g_{n_2} && \text{since } n_2 - n_1 = k \\
&= a_{n_1} + n_1 + k - 1 - n_1 + g_{n_2} && \text{by (2)} \\
&= a_{n_1} + k - 1 + g_{n_2} \\
&= rn_1 + k - 1 + g_{n_2} && \text{by hypothesis since } a_{n_1} = rn_1 \\
&= (rn_1 + k - 1) + ((r-1)k + 1) \\
&= r(n_1 + k) \\
&= rn_2
\end{aligned}$$

Thus, (c) holds. □

We can immediately obtain the following result for $a_1 = 7$.

Theorem 4. *Let $a_1 = 7$. For each $n \geq 2, a_n - a_{n-1}$ is 1 or prime.*

Proof. We compute the first few terms of the a_n and g_n sequences and obtain

$$a_1 = 7,\ a_2 = 8,\ a_3 = 9$$
$$g_2 = 1,\ g_3 = 1$$

Let $n_1 = 3$. Notice that $a_3 = 3 \cdot n$. Let n_2 be the smallest integer greater than 3 such that $g_{n_2} \neq 1$. Thus, we take $r = 3$ in Lemma 1, and note that $n_2 > 3 > \frac{3}{r-1}$. By the Lemma, g_{n_2} is prime, and $a_{n_2} = 3n_2$. Now let n_3 be the next largest integer such that $g_{n_3} \neq 1$. By the Lemma again, g_{n_3} is prime and $a_{n_3} = 3n_3$. Continuing, we get that g_n is always 1 or prime. □

5 Further Explorations

The next natural question is what happens if the initial condition is changed? Consider when $a_1 = 8$. We can generate the sequence using Mathematica. The first few primes of g_n after 100,000 iterations and discarding the ones are

2, 7, 13, 5, 29, 3, 59, 3, 7, 5, 3, 131, 3, 263, 3, 17, 3, 5, 3, 19, 569, 3, 17, 3, 13, 7, 5, 3, 1181, 3, 17, 3, 2381, 3, 11, 3, 5, 3, 7, 4787, 3, 5, 3, 11, 3, 53, 3, 11, 3, 13, 19, 9689, 3,19379, 3, 7, 5, 3, 137, 3, 13, 38921, 3, 17, 3, 7, 77867, 3, 5, 3, $\cdots$

Now consider when $a_1 = 15$. We have the sequence

13, 5, 29, 3, 59, 3, 7, 5, 3, 131, 3, 263, 3, 17, 3, 5, 3, 19, 569, 3, 17, 3, 13, 7, 5, 3, 1181, 3, 17, 3, 2381, 3, 11, 3, 5, 3, 7, 4787, 3, 5, 3, 11, 3, 53, 3, 11, 3, 13, 19, 9689, 3, 19379, 3, 7, 5, 3, 137, 3, 13, 38921, 3, 17, 3, 7, 77867, 3, 5, 3, $\cdots$

Consider when $a_1 = 25$. We have the sequence

23, 3, 47, 3, 5, 3, 101, 3, 7, 11, 3, 13, 233, 3, 467, 3, 5, 3, 941, 3, 7, 1889, 3, 3779, 3, 7559, 3, 13, 15131, 3, 53, 3, 7, 30323, 3, 60647, 3, 5, 3, 101, 3 $\cdots$

After experimentation, it appears that g_n is 1 or prime for every initial condition. In [5], it is stated that most small inital conditions quickly produce a state in which the Lemma applies. In the previous section, we proved that the difference sequence will always produce primes as long as $a_n/n = 2$ or 3 whenever $g_n \neq 1$. Rowland mentions in [5] that the small initial conditions not covered by the proof of the Lemma are $a_2 = 4$, $a_1 = 3$, and $a_1 = 2$.

References

[1] B. Bischof, J. Gomez-Calderon, and A. Perriello, *Integer-coeffiecient polynomials have prime-rich images.*, Math. Mag. **(83)**, 2010, 55-57.

[2] M. Erickson and T. Vazzana, *Introduction to Number Theory.*Chapman & Hall/CRC Press, New York, 2008.

[3] E. Pegg Jr., *Math Games: Prime Generating Polynomials*, MAA, 2006,
http://www.maa.org/editorial/mathgames/mathgames_07_17_06.html

[4] P. Ribenboim, *Are there Functions that Generate Prime Numbers?*, College Math. J. **(28)**, no. 5, 1997, 352-359.

[5] E. Rowland, *A Natural Prime-Generating Recurrence*, J. Integer Seq. **11** (2008) no. 2, Article 08.2.8.