



PRIME VALUES OF SOME FAST GROWING SEQUENCES

Andrew Granville

Department of Mathematics, Université de Montréal, Montréal, Québec, Canada
 andrew.granville@umontreal.ca

Received: 10/27/25, Accepted: 2/26/26, Published: 9/28/26

Abstract

We survey one and two dimensional covering systems, primarily concerned with how often sequences like $\{a \cdot 2^n + b\}_{n \geq 1}$ and $\{a^m - b^n\}_{m, n \geq 1}$ take on prime values.

Celebrating the 80th Birthdays of Mel Nathanson and Carl Pomerance

For those of us who are fascinated by combinatorial and by addi(c)tive number theory, the works of both Mel and Carl hold a special place. Mel has been a champion of additive combinatorics since before the subject had a name, writing his classic books [12, 13] which are still in many ways the best and most inspiring references, as well as creating some of the fundamental questions (e.g., [11]) that have flowered into so much today. Carl has worked with combinatorial and analytic methods in all sorts of novel ways, most famously to understand the running times of number theoretic algorithms [2], but also has a love of fundamental problems, especially about primes and sequences.

No two people have continued on the mathematical legacy of Paul Erdős as much as Mel and Carl with such open-handed intellectual generosity, and encouraged so many others to share in the joy of understanding such questions. A warm thank you to them both.

1. Primes in Sparse, Naturally Occurring, Sequences

1.1. Mersenne Primes and Fibonacci Primes

Once you have started playing with the Fibonacci numbers $\{F_n\}_{n \geq 1}$ or the Mersenne numbers, $\{2^n - 1\}_{n \geq 1}$, then you find yourself asking how often they are prime: Are Mersenne numbers prime as often **AS** regular integers or do we need some special

understanding (after all, they are a very special sequence of numbers) to determine how often they are prime? Let's look at the data for small n :

$$\begin{aligned} 2^n - 1 \text{ is prime for } n &= 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, \dots;^1 \\ F_n \text{ is prime for } n &= 3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 83, \dots.^2 \end{aligned}$$

We immediately observe that in both cases these n are all prime powers (and, in fact, all prime except for $n = 4$). This is always true:

We observe that $2^m - 1$ always divides $2^n - 1$ if m divides n and that the sequence is increasing. Therefore $2^n - 1$ is composite whenever n is composite. Put another way, if $2^n - 1$ is prime then n is prime.

A similar argument works for the Fibonacci numbers since F_m divides F_n whenever m divides n , though we have to be a little more careful as they begin $F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2$ so are only increasing for $n \geq 2$. Thus if $n = ab$ with $a, b > 1$ then F_n is composite provided $F_a, F_b > 1$, that is, if $a > 2$ or $b > 2$. We deduce that if F_n is prime then n is prime or $n = 4$.

We might guess that each of these lists can be extended to infinitely many prime values in each sequence, but we know of no way to prove it and even struggle to obtain much data since each of these sequences grows exponentially quickly. Nonetheless, to get a better feeling for this question we can try to construct a heuristic for how many such primes there are and feel some confidence if our heuristic fits reasonably with the available data.

1.2. Primes of the Form $k \cdot 2^n - 1$, with $k > 1$ Odd

Here are the first few n -values for which $k \cdot 2^n - 1$ is prime, with $k > 1$ odd:

$k = 3$: Primes for $n = 1, 2, 3, 4, 6, 7, 11, 18, 34, 38, 43, 55, 64, 76, 94, \dots$

$k = 5$: Primes for $n = 2, 4, 8, 10, 12, 14, 18, 32, 48, 54, 72, \dots$

$k = 7$: Primes for $n = 1, 5, 9, 17, 21, 29, 45, \dots$

$k = 9$: Primes for $n = 1, 3, 7, 13, 15, 21, 43, 63, 99, \dots$

Based on this scanty evidence we might guess that there are infinitely primes in each of these sequences, but again we cannot calculate too far since each of these sequences grows exponentially quickly.

¹The list continues beyond 100: 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 42643801, 43112609, 57885161, 74207281, 77232917, 82589933, 136279841; so far 52 Mersenne primes are known.

²The list continues beyond 100: 131, 137, 359, 431, 433, 449, 509, 569, 571, 2971, 4723, 5387, 9311, 9677, 14431, 25561, 30757, 35999, 37511, 50833, 81839, 104911, 130021, 148091, 201107; so far 37 Fibonacci primes are known. In addition there are 20 more Fibonacci numbers that are probable primes: 397379, 433781, 590041, 593689, 604711, 931517, 1049897, 1285607, 1636007, 1803059, 1968721, 2904353, 3244369, 3340367, 4740217, 6530879, 7789819, 10317107, 10367321, 11964299.

These are quite different from the prime values of $2^n - 1$ since not all these n -values are primes. Nonetheless can we discern any patterns amongst these n -values? I do not think anything is too obvious, but let's try to adapt what we know about prime values of polynomials:

1.3. Prime Values in Arithmetic Progressions of n -values, for Polynomials and for Linear Recurrences

Let $f(x) \in \mathbb{Z}[x]$. Gauss showed that if $a \equiv b \pmod{m}$ then $f(a) \equiv f(b) \pmod{m}$. That is, $f(n) \pmod{m}$ is periodic mod m as n varies. In particular this implies that there is a set of residues $R_m \pmod{m}$ such that m divides $f(a)$ if and only if a belongs to certain arithmetic progressions mod m ; that is, if $a \equiv r \pmod{m}$ for some $r \in R_m$. Thus, for example,

$$\begin{aligned} 5 \text{ divides } n^2 + 1 \text{ if and only if } n \equiv 2 \text{ or } 3 \pmod{5} \\ \text{and} \\ 13 \text{ divides } n^2 + 1 \text{ if and only if } n \equiv 5 \text{ or } 8 \pmod{13}. \end{aligned}$$

Therefore $(n^2 + 1, 5) = 1$ for 3 residue classes mod 5, and $(n^2 + 1, 13) = 1$ for 11 residue classes mod 13, so that $(n^2 + 1, 5 \cdot 13) = 1$ for 33 residue classes mod 65, by the Chinese Remainder Theorem. That is, $(n^2 + 1, 5 \cdot 13) > 1$ for 32 residue classes mod 65. One can continue such an analysis for arbitrarily many primes. In fact, if prime $p \equiv 1 \pmod{4}$ then

$$p \text{ divides } n^2 + 1 \text{ if and only if } n \text{ is in one of two residue classes mod } p$$

and so if $p_1 < p_2 < \dots < p_k$ are distinct primes $\equiv 1 \pmod{4}$ then $(n^2 + 1, p_1 \dots p_k) = 1$ for only $\prod_{j=1}^k (p_j - 2)$ residue classes mod $p_1 \dots p_k$.

For linear recurrences it is also true that if a prime p divides $k \cdot 2^n - 1$ for some value of n , then it divides $k \cdot 2^n - 1$ in arithmetic progressions of n -values though here identifying the modulus of the arithmetic progression is not so straightforward. Let $m > 1$ be an integer with $(m, 2k) = 1$, and let r be the order of 2 mod m . Then

$$k \cdot 2^{n+r} - 1 = k \cdot 2^n \cdot 2^r - 1 \equiv k \cdot 2^n - 1 \pmod{m}$$

and so the sequence $k \cdot 2^{n+r} - 1 \pmod{m}$ is periodic with period r , and, in fact, r is the smallest period. It is not always easy to identify r , the order of 2 mod m , but we know from Euler's Theorem that r always divides $\phi(m)$ and so $k \cdot 2^{n+\phi(m)} - 1 \pmod{m}$ is periodic. Thus for example

$$\begin{aligned} 5 \text{ divides } 3 \cdot 2^n - 1 \text{ if and only if } n \equiv 1 \pmod{4} \\ 11 \text{ divides } 3 \cdot 2^n - 1 \text{ if and only if } n \equiv 2 \pmod{10} \end{aligned}$$

When we try to combine these congruences, we find that things now differ significantly from the polynomial case since it is evident that 5 and 11 cannot both divide

$3 \cdot 2^n - 1$ (as n cannot be both odd and even!). We see that the arithmetic progressions for the n -values are no longer necessarily independent, we cannot use the Chinese Remainder Theorem, and this makes understanding small prime divisors much more challenging.

On the other hand, Paul Erdős realized that these incompatible congruences could be leveraged to construct such exponentially growing sequences which contain no primes at all.

2. Using Covering Systems to Avoid Prime Values

In 1934 Romanoff [16] proved that a positive proportion of odd integers *can* be written in the form $2^k + p$ where p is prime and k is an integer greater than or equal to 1. It was conjectured that perhaps this was true for every sufficiently large odd integer. However, Erdős [3] disproved this conjecture in an extraordinary way: to show that an odd integer m *cannot be written* as $2^k + p$, is equivalent to showing that $m - 2^k$ is composite whenever $2^k < m - 1$. In fact, Erdős proved more: there exists an arithmetic progression of odd integers $a \pmod{d}$ and an integer Q such that if $m \equiv a \pmod{d}$ then

$$(m - 2^k, Q) > 1 \text{ for all integers } k \geq 0.$$

Therefore if $m - 2^k$ is prime, its value must be a prime divisor of Q , that is, $m = p + 2^k$ where p divides Q , and evidently the number of such $m \leq x$ is $\leq \omega(Q) \cdot \frac{\log x}{\log 2}$ where $\omega(Q)$ is the number of distinct prime divisors of Q , which is far smaller than the number of $m \leq x$ with $m \equiv a \pmod{d}$. Therefore Erdős was able to deduce that a positive proportion of odd integers *cannot* be written in the form $2^k + p$ where p is prime and k is an integer greater than or equal to 1.

It is still an open question as to exactly what is the proportion of odd integers that can be written in the form $2^k + p$ (and even whether a limiting proportion exists; after all, it is feasible that the proportion oscillates between two distinct quantities, all the way out to infinity). Under certain reasonable assumptions we do know that, in the limit, the proportion is between $0.6154\dots$ and $0.9818\dots$ so we are a long way from pinning this down.

2.1. The Original Covering System of Paul Erdős [3]

We select $a \pmod{Q}$ where $Q = 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$ using the Chinese Remainder Theorem, where

$$a \equiv 2^0 \pmod{21}, 2^1 \pmod{5}, 2^3 \pmod{17}, 2^7 \pmod{13}, 2^{23} \pmod{241}.$$

Therefore if $m \equiv a \pmod{Q}$ then the following hold:

- If $n \equiv 0 \pmod{2}$ then $m - 2^n \equiv a - 2^0 \equiv 0 \pmod{3}$;
- If $n \equiv 0 \pmod{3}$ then $m - 2^n \equiv a - 2^0 \equiv 0 \pmod{7}$;
- If $n \equiv 1 \pmod{4}$ then $m - 2^n \equiv a - 2^1 \equiv 0 \pmod{5}$;
- If $n \equiv 3 \pmod{8}$ then $m - 2^n \equiv a - 2^3 \equiv 0 \pmod{17}$;
- If $n \equiv 7 \pmod{12}$ then $m - 2^n \equiv a - 2^7 \equiv 0 \pmod{13}$;
- If $n \equiv 23 \pmod{24}$ then $m - 2^n \equiv a - 2^{23} \equiv 0 \pmod{241}$.

Therefore $(m - 2^n, 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241) > 1$ for all integers $n \geq 0$, since every integer $n \geq 0$ satisfies at least one of the given congruences for n . This set of congruences for n is called a *covering system*. We deduce that the proportion of odd integers m that cannot be represented as $p + 2^k$ is at least $\frac{1}{Q}$.

2.2. Different Questions, Same Covering System

Select a and Q as in the previous subsection. Note that $(a, Q) = 1$ by construction.

1. Let $b \equiv -a \pmod{Q}$. If $m \equiv b \pmod{Q}$ then $m + 2^n \equiv b + 2^n \equiv -(a - 2^n) \pmod{Q}$ and so $(m + 2^n, Q) = (a - 2^n, Q) > 1$ for every integer $n \geq 0$. Thus for all but a few $m \equiv b \pmod{Q}$ there are no primes of the form $m + 2^n$.
2. Let $c \equiv a^{-1} \pmod{Q}$. If $m \equiv c \pmod{Q}$ then $a(m \cdot 2^n - 1) \equiv ac \cdot 2^n - a \equiv -(a - 2^n) \pmod{Q}$ and so $(m \cdot 2^n - 1, Q) = (a - 2^n, Q) > 1$ for each $n \geq 0$. So for all but a few $m \equiv c \pmod{Q}$ there are no primes of the form $m \cdot 2^n - 1$.
3. Let $d \equiv -a^{-1} \pmod{Q}$. If $m \equiv d \pmod{Q}$ then $a(m \cdot 2^n + 1) \equiv ad \cdot 2^n + a \equiv a - 2^n \pmod{Q}$ and so $(m \cdot 2^n + 1, Q) = (a - 2^n, Q) > 1$ for each $n \geq 0$. So for all but a few $m \equiv d \pmod{Q}$ there are no primes of the form $m \cdot 2^n + 1$.
4. This case generalizes all four earlier ones. Suppose ℓ and m are odd coprime integers with $\ell \equiv -am \pmod{Q}$ and $(m, Q) = 1$. Then $\ell + m \cdot 2^n \equiv (-m)(a - 2^n) \pmod{Q}$ and so $(\ell + m \cdot 2^n, Q) = (a - 2^n, Q) > 1$ for each $n \geq 0$. So $\ell + m \cdot 2^n$ is composite for all $n \geq 0$ other than perhaps for a few values which equal the prime divisors of Q .

Suppose that $(\ell + m \cdot 2^n, Q) > 1$ for each $n \geq 0$. For each prime p dividing Q let $m_p = \text{ord}_p(2)$ and let a_p be the minimal positive integer for which p divides $\ell + m \cdot 2^{a_p}$. Then p divides $\ell + m \cdot 2^n$ if and only if $n \equiv a_p \pmod{m_p}$ and so $(\ell + m \cdot 2^n, Q) > 1$ for each $n \geq 0$ if and only if $\cup_{p|Q} \{n \in \mathbb{Z} : n \equiv a_p \pmod{m_p}\} = \mathbb{Z}$.

2.3. Riesel's Use of Fermat Numbers

In 1956, Riesel [15] gave an elegant construction of a covering system based on what we know about Fermat numbers. The *Fermat numbers* are the integers $F_n = 2^{2^n} + 1$. Fermat noted that $F_0, \dots, F_4$ are all primes but Euler observed that $F_5 = pq$ where $p = 641$ and $q = 6700417$. We now use the Chinese Remainder Theorem to construct a congruence class $a \pmod{Q}$ where $Q = F_0 \cdots F_5 = 2^{2^6} - 1$ and a is given by

$$a \equiv -1 \pmod{F_0 F_1 F_2 F_3 F_4 p} \text{ and } a \equiv 1 \pmod{q}.$$

We will use the fact that

$$2^{2^{n+1}} \equiv 1 \pmod{F_n}.$$

Therefore if $m \equiv a \pmod{Q}$ then the following hold:

- If $n \equiv 2^0 \pmod{2^1}$ then $m \cdot 2^n - 1 \equiv -2^{2^0} - 1 \equiv 0 \pmod{F_0}$;
- If $n \equiv 2^1 \pmod{2^2}$ then $m \cdot 2^n - 1 \equiv -2^{2^1} - 1 \equiv 0 \pmod{F_1}$;
- If $n \equiv 2^2 \pmod{2^3}$ then $m \cdot 2^n - 1 \equiv -2^{2^2} - 1 \equiv 0 \pmod{F_2}$;
- If $n \equiv 2^3 \pmod{2^4}$ then $m \cdot 2^n - 1 \equiv -2^{2^3} - 1 \equiv 0 \pmod{F_3}$;
- If $n \equiv 2^4 \pmod{2^5}$ then $m \cdot 2^n - 1 \equiv -2^{2^4} - 1 \equiv 0 \pmod{F_4}$;
- If $n \equiv 2^5 \pmod{2^6}$ then $m \cdot 2^n - 1 \equiv -2^{2^5} - 1 \equiv 0 \pmod{p}$;
- If $n \equiv 0 \pmod{2^6}$ then $m \cdot 2^n - 1 \equiv 2^0 - 1 \equiv 0 \pmod{q}$.

Therefore $(m \cdot 2^n - 1, Q) > 1$ for all integers $n \geq 0$.

Let $b \equiv -a \pmod{Q}$. In 1960 Sierpiński [18] showed that if $m \equiv b \pmod{Q}$ then $(m \cdot 2^n + 1, Q) > 1$ for all integers $n \geq 0$. A proof follows from Riesel's construction and then part 1 in the previous subsection.

3. Two-Dimensional Covering Systems to Avoid Prime Values

Francesco Pappalardi and I [6] recently observed that

$$(41^m - 34^n, 3 \cdot 5 \cdot 7) > 1 \text{ for all integers } m, n \geq 0.$$

Notice that this can be prime as $41^1 - 34^1 = 7$, but it can only be prime finitely often. We now see how and why this works:

$$41^m - 34^n \equiv \begin{cases} (-1)^m - 1 & \pmod{3}, \text{ so is divisible by 3 if } m \equiv 0 \pmod{2}; \\ 1 - (-1)^n & \pmod{5}, \text{ so is divisible by 5 if } n \equiv 0 \pmod{2}; \\ (-1)^m - (-1)^n & \pmod{7}. \text{ so is divisible by 7 if } m \equiv n \pmod{2}. \end{cases}$$

These congruences for m and n cover all pairs of integers m, n so we call them a *two-dimensional covering system*. This raises the question of how this generalizes.

3.1. A General Two-Dimensional Covering System for $a^m - b^n$ Using Order Two Elements

Suppose that p, q, r are three distinct odd primes, with

$$\begin{aligned} a &\equiv -1 \pmod{p} \text{ and } b \equiv -1 \pmod{p}, \\ a &\equiv 1 \pmod{q} \text{ and } b \equiv -1 \pmod{q}, \text{ and} \\ a &\equiv -1 \pmod{r} \text{ and } b \equiv -1 \pmod{r}. \end{aligned}$$

Then $(a^m - b^n, p \cdot q \cdot r) > 1$ for all integers $m, n \geq 0$.

This means that if $a^m - b^n$ is prime then it equals p, q or r . This may happen (as in the previous subsection) but one can show that there are only finitely many (m, n) for which $a^m - b^n$ is a prime power, using results on S -unit equations.

The key to this construction is the covering system for (m, n) -pairs, and the fact that $a^2 \equiv b^2 \equiv 1$ modulo each of p, q and r . What if we try with $a^3 \equiv b^3 \equiv 1$ modulo each prime factor of Q ?

3.2. Two-Dimensional Covering System Using Order Three Elements

If prime p is congruent to 1 (mod 3), then there are two residue classes mod p of order 3. When we write $b^3 \equiv' 1 \pmod{p}$ we mean that we select $b \pmod{p}$ to have order 3. Suppose that p, q, r, s are four distinct odd primes $\equiv 1 \pmod{3}$, and

$$\begin{aligned} a &\equiv 1, \quad b^3 \equiv' 1 \pmod{p} \text{ so that } p \mid a^m - b^n \text{ if } n \equiv 0 \pmod{3}; \\ a^3 &\equiv' 1, \quad b \equiv 1 \pmod{q} \text{ so that } q \mid a^m - b^n \text{ if } m \equiv 0 \pmod{3}; \\ a &\equiv b, \quad b^3 \equiv' 1 \pmod{r} \text{ so that } r \mid a^m - b^n \text{ if } m \equiv n \pmod{3}; \\ a &\equiv b^2, \quad b^3 \equiv' 1 \pmod{s} \text{ so that } s \mid a^m - b^n \text{ if } m \equiv -n \pmod{3}. \end{aligned}$$

Then $(a^m - b^n, p \cdot q \cdot r \cdot s) > 1$ for all integers $m, n \geq 0$.

For example let $a = 15226$ and $b = 67419$ with $p = 7, q = 13, r = 19, s = 31$ so that

$$(15226^m - 67419^n, 7 \cdot 13 \cdot 19 \cdot 31) > 1 \text{ for all integers } m, n \geq 0.$$

How much further can we generalize this?

3.3. How to Identify When $(a^m - b^n, Q) > 1$ For All Integers $m, n \geq 0$

For each prime p dividing Q we can determine for what (m, n) -values p divides $a^m - b^n$ as follows.

Lemma 1. *Let $L = L_p := [r, s]$ where $r = \text{ord}_p(a), s = \text{ord}_p(b)$ and $u_p = \frac{r}{(r, s)}$. There is a unique $v_p \pmod{s}$ such that $a^{u_p} \equiv b^{v_p} \pmod{p}$. Moreover $a^m \equiv b^n \pmod{p}$ if and only if $mv_p \equiv nu_p \pmod{L_p}$.*

We can then deduce that $(a^m - b^n, Q) > 1$ for all integers $m, n \geq 0$ if and only if the set of congruences

$$\{(m, n \in \mathbb{Z} : mv_p \equiv nu_p \pmod{L_p})\}_{p|Q}$$

covers all integer pairs $(m, n) \in \mathbb{Z}^2$.

Proof of Lemma 1. Let $u_p = \frac{r}{(r,s)}, w_p = \frac{s}{(r,s)}$ and

$$A = a^{u_p}, B = b^{w_p} \text{ so that } \text{ord}_p(A) = \text{ord}_p(B) = (r, s).$$

Then $A \equiv B^t \pmod{p}$ for some unique $t \pmod{(r, s)}$, and let $v_p = tw_p$, so v_p is unique mod s and $a^{u_p} = A \equiv B^t = b^{tw_p} = b^{v_p} \pmod{p}$. Note also that $(u_p, w_p) = 1$.

Now suppose that $a^m \equiv b^n \pmod{p}$. Then $(a^m)^r = (a^r)^m \equiv 1 \pmod{p}$ and $(a^m)^s \equiv (b^n)^s \equiv (b^s)^n \equiv 1 \pmod{p}$, and so $(a^m)^{(r,s)} \equiv (b^n)^{(r,s)} \equiv 1 \pmod{p}$. Therefore $u_p \mid m$ and $v_p \mid n$ and we write $m = u_p M, n = v_p N$ so that $A^M = a^m \equiv b^n = B^N \pmod{p}$. This in turn implies that $N \equiv tM \pmod{(r, s)}$. We multiply this through by $u_p w_p$ to obtain $nu_p \equiv mv_p \pmod{L := [r, s]}$.

In the other direction, if $nu_p \equiv mv_p \pmod{L}$ then $u_p \mid m, w_p \mid n$ as $u_p w_p \mid L$. Writing $m = u_p M, n = w_p N$ and dividing through by $u_p w_p$ yields $N \equiv tM \pmod{(r, s)}$ and so $b^n = B^N \equiv B^{tM} \equiv A^M = a^m \pmod{(r, s)}$. $\square$

3.4. Constructing Two-Dimensional Covering Systems

Following up on the previous subsection, we begin with a 2-dimensional covering system

$$\bigcup_{1 \leq j \leq k} \{(m, n) \in \mathbb{Z}^2 : mv_j \equiv nu_j \pmod{L_j}\} = \mathbb{Z}^2$$

where each $(u_j, v_j, L_j) \in \mathbb{Z}_{\geq 1}^3$ with $u_j \mid L_j$ and $(u_j, v_j) = 1$.

We select distinct primes $p_j \equiv 1 \pmod{L_j}$. Let g_j be a residue of order L_j mod p_j and select $a \equiv g^{v_j}, b \equiv g^{u_j} \pmod{p_j}$ for each j (via the Chinese Remainder Theorem), so that $a^{u_j} \equiv g^{u_j v_j} \equiv b^{v_j} \pmod{p_j}$. We can then use Lemma 1 to establish that

$$a^m \equiv b^n \pmod{p} \text{ if and only if } mv_j \equiv nu_j \pmod{L_j}.$$

Therefore if $Q = p_1 \cdots p_k$ then

$$(a^m - b^n, Q) > 1 \text{ for all integers } m, n \geq 0.$$

The examples in the subsections above are specific cases of this construction.

3.5. Observations about Two-Dimensional Covering Systems

Let $(u, v; L)$ be an abbreviation for $\{(m, n) \in \mathbb{Z}^2 : mv \equiv nu \pmod{L}\}$.

1. We now show that any 2-d congruence is equivalent to one with $u \mid L$ and $(u, v) = 1$: We first note that $(u, v; L) = (gu, gv; gL)$ for any $g \geq 1$ so we can assume $\gcd(u, v, L) = 1$ without loss of generality. Now, if $r = \gcd(u, v)$ then $(r, L) = 1$ and so $(u, v; L) = (u/r, v/r; L)$ and so we can assume that $\gcd(u, v) = 1$. If $d = \gcd(u, L)$ then write $u = ds$ so that $(s, L/d) = 1$ and therefore there exists t with $st \equiv 1 \pmod{L/d}$. Therefore $(u, v; L) = (d, vt; L)$. Hence we may assume that $u \mid L$.

Let $\mathcal{C} = \{(u_j, v_j; L_j) : 1 \leq j \leq k\}$ be a 2-d covering system where $u_j \mid L_j$ and $(u_j, v_j) = 1$ for each j and define $L = [L_j : 1 \leq j \leq k]$.

2. If $(m, L) = 1$ and $mv_j \equiv nu_j \pmod{L_j}$ then (u_j, L_j) divides mv_j , and so (u_j, L_j) divides (u_j, L_j, mv_j) , which divides $(L, m)(u_j, v_j) = 1$ and so $(u_j, L_j) = 1$. But $u_j \mid L_j$ as well, so $u_j = 1$. Therefore the subset $\mathcal{C}' := \{(1, v; L) \in \mathcal{C}\}$ covers all pairs of integers (m, n) with $\gcd(m, L) = 1$. Taking $m = 1$ this implies that the set of congruences $\{v_j \pmod{L_j} : u_j = 1\}$ is a 1-d covering system.

3. For any pair of integers m, n with $\gcd(m, n) = g > 1$, we can take $M = m/g, N = n/g$, so that $a^M - b^N$ divides $a^m - b^n$ and so $a^m - b^n$ is typically composite if $\gcd(m, n) > 1$. This suggests looking only for sets of congruences $\mathcal{C}$ that cover all pairs of integers (m, n) with $\gcd(m, n) = 1$. However, we now show that such sets of congruences are actually 2-d covering systems.

Suppose that $\mathcal{C} = \{(u_j, v_j; L_j) : 1 \leq j \leq k\}$ is a set of congruences that covers all pairs of integers (m, n) with $\gcd(m, n) = 1$. If $\gcd(m, n) = g$ with $g > 1$ then let $M = m/g, N = n/g$ so there exists j such that $Mv_j \equiv Nu_j \pmod{L_j}$. Multiplying through by g we deduce that $mv_j \equiv nu_j \pmod{L_j}$. Therefore $\mathcal{C}$ is a 2-d covering system.

4. Cochrane and Myerson [1] showed that there exists a 2-d covering system $(u_j, v_j; L_j)$ where the L_j are all distinct.

4. Incomplete 1-d Covering Systems

An *incomplete 1-d covering system* for the sequence $\ell \cdot 2^n + m$ is given by a set of congruences for which $(\ell \cdot 2^n + m, Q) > 1$ if n satisfies one of these congruences, together with the property that $\ell \cdot 2^n + m$ has an algebraic factor (given by a formula) for all remaining n .

For example, imagine there is a set of arithmetic progressions $\{a_i \pmod{m_i}\}$ which cover the odd integers, such that if $n \equiv a_i \pmod{m_i}$ then prime p_i divides $r^2 \cdot 2^n - 1$. Then $(r^2 \cdot 2^n - 1, Q) > 1$ for all odd integers $n \geq 1$ where $Q = p_1 \cdots p_k$. For even $n = 2N$ we know that $r \cdot 2^N - 1$ divides $r^2 \cdot 2^n - 1$, so $r^2 \cdot 2^n - 1$ can be prime for only finitely many integers n . We do not know such a set of arithmetic progressions (along with the p_i), but it is plausible that this is doable.

4.1. Izotov's Construction

The last idea can work in an analogous setting as first shown by Izotov [9] in 1995: As in Section 2.3, let $F_n = 2^{2^n} + 1$ and $F_5 = pq$. We construct $a \pmod{Q}$ where $Q = F_0 F_2 F_3 F_4 F_5$ and a is given by

$$a \equiv 1 \pmod{F_0 F_2 F_3 F_4 p} \text{ and } a \equiv 2^{2^3} \pmod{q}.$$

and so if $m = a^4$ then

$$m \equiv 1 \pmod{F_0 F_2 F_3 F_4 p} \text{ and } m \equiv 2^{2^5} \equiv -1 \pmod{q}.$$

Proceeding as in Section 2.3 we deduce that $(m \cdot 2^n + 1, Q) > 1$ for all integers n except those that are $\equiv 2 \pmod{4}$.³ Writing $n = 4k + 2$ for any remaining n we have

$$m \cdot 2^n + 1 = a^4 \cdot 2^{4k+2} + 1 = (a^2 \cdot 2^{2k+1} + a \cdot 2^{k+1} + 1)(a^2 \cdot 2^{2k+1} - a \cdot 2^{k+1} + 1)$$

which is obviously composite. We remark that if $5 \nmid a$ then $m \equiv 1 \pmod{5}$ and we get the same covering system as in Section 2.3. To avoid this we select $a \equiv 0 \pmod{5}$.

4.2. Erdős's Conjecture

We do not know for sure that $\{m \cdot 2^n + 1 : n \geq 0\}$ cannot be covered by a covering system in the last subsection but we doubt it. If not then Izotov's construction disproves a conjecture of Erdős [8, section F13] that if $\{m \cdot 2^n + 1, n \geq 0\}$ contains only finitely many primes then there exists an integer Q for which $(m \cdot 2^n + 1, Q) > 1$. So Filaseta, Finch and Kozek [4] suggested in 2008 modifying Erdős's conjecture by adding the condition that m is not a perfect power.

4.3. Variations on the Theme

There are many alternative constructions, and variations on this theme charmingly discussed and developed by Filaseta, Finch and Kozek [4].

³In the construction in Section 2.3 we had 5 dividing $m \cdot 2^n + 1$ when $m \equiv 2 \pmod{4}$, but here we avoided specifying $a \pmod{F_1 = 5}$.

The key to Izotov’s construction is that $4x^4 + 1$ factors as a polynomial into two polynomials of degree two, so when we substitute $x = 2^k a$ we get a factorization of $a^4 2^{4k+2} + 1$ into two fairly large integers.

This generalizes to the so-called *Aurefeuillean factorizations* of integers of the form $b^n \pm 1$, algebraic factorizations of such integers for the n -values in certain special arithmetic progressions. First identified as interesting by Gauss, this was extended by certain authors through to Schinzel [17] in 1962, and in 2006 Granville and Pleasants [7] explained why Schinzel’s list is almost certainly complete.

4.4. Proving That There Is No Covering System

Filaseta, Finch and Kozek [4] showed that for any integer Q there are integers n for which $(3 \cdot 2^n + 1, Q) = 1$, and therefore there can be no covering system for $3 \cdot 2^n + 1$. More generally let a and b be given coprime, odd integers. Then $a \cdot 2^n + b$ is odd for all $n \geq 1$. Suppose that Q is an odd integer. By Euler’s Theorem we know that if $\phi(Q)$ divides n then $2^n \equiv 1 \pmod{Q}$. But then $a \cdot 2^n + b \equiv a + b \pmod{Q}$ so that $(a \cdot 2^n + b, Q) = (a + b, Q)$. In particular if $a + b = \pm 2^r$ for some integer $r \geq 1$ then there can be no integer Q for which $(a \cdot 2^n + b, Q) > 1$ for all integers $n \geq 1$.

5. How Many Prime Values Are There in a Given Sparse Sequence?

Suppose that there are infinitely many primes amongst $\{m \cdot 2^n + 1\}_{n \geq 1}$. We would like to predict how many prime values there are in the set $\{m \cdot 2^n + 1 : 1 \leq n \leq x\}$, at least if x is sufficiently large. In this Section we will develop some heuristics, modifying well-established predictions about prime values of polynomials. The conjectures about polynomials are backed-up with a large amount of data, as well as proofs “on average”.

5.1. Gauss’s “One in Every $\log x$ ” Prediction

When Gauss was a teenager he counted primes in intervals of length 1000. For example, he obtained the data in Table 1:

m	0	1	2	3	4	5	6	7	8	9
# primes	168	135	127	120	119	114	117	107	110	112

Table 1: Number of primes in $(m \cdot 10^3, (m + 1) \cdot 10^3)$.

From these counts Gauss guessed that the density of primes near x is roughly inversely proportional to $\log x$, so the number of primes in $(m \cdot 10^3, (m + 1) \cdot 10^3)$

should be about
$$\int_{m \cdot 10^3}^{(m+1) \cdot 10^3} \frac{dt}{\log t}.$$

m	0	1	2	3	4	5	6	7	8	9
# primes	168	135	127	120	119	114	117	107	110	112
GAUSS	178	137	128	123	119	116	114	112	111	109

Table 2: Prime counts vs. Gauss's $\int_{m \cdot 10^3}^{(m+1) \cdot 10^3} \frac{dt}{\log t}$.

Gauss's guesses in Table 2 look pretty accurate, and suggests that, in general,

$$\pi(x) := \sum_{\text{primes } p \leq x} 1 \approx \int_2^x \frac{dt}{\log t} := \text{Li}(x).$$

Table 3 presents the latest data on that.

x	$\pi(x) := \#\{\text{primes} \leq x\}$	Overcount: $\text{Li}(x) - \pi(x)$
10^6	78498	130
10^9	50847534	1701
10^{12}	37607912018	38263
10^{15}	29844570422669	1052619
10^{18}	24739954287740860	21949555
10^{19}	234057667276344607	99877775
10^{20}	2220819602560918840	222744644
10^{21}	21127269486018731928	597394254
10^{22}	201467286689315906290	1932355208
10^{23}	1925320391606803968923	7250186216
10^{24}	18435599767349200867866	17146907278
10^{25}	176846309399143769411680	55160980939
10^{26}	1699246750872437141327603	155891678121
10^{27}	16352460426841680446427399	508666658006
10^{28}	157589269275973410412739598	1427745660374
10^{29}	1520698109714272166094258063	4551193622464

Table 3: Primes up to x 's $\leq 10^{29}$, and overcount in Gauss's prediction

The “take-away” from all this is that if we randomly select integers near to x , then about 1 in every $\log x$ will be prime; a heuristic mused by Gauss in a letter on Christmas Eve of 1849.

In this article we are concerned with randomly selecting integers near x from some algebraically defined subsequence, and asking how many of these are prime?

5.2. Prime Values in a Sparse Set of Integers

Let $\mathcal{A}$ be a set of integers and $A(x) = \#\{a \in \mathcal{A} : a \leq x\}$. Assuming that $A(x)$ grows in some uniform way with respect to x , the usual heuristic guesses that the number

of primes, $\pi_{\mathcal{A}}(x)$, in $\mathcal{A}$ up to x , is $\sim c_{\mathcal{A}} \frac{A(x)}{\log x}$ where $c_{\mathcal{A}}$ depends on the distribution of $\mathcal{A}$ with respect to small primes.

For example, if $\mathcal{A}_k = \{n : n + k \text{ is prime}\}$ for each $k \geq 1$ then we see a big difference between k odd and k even, so we need to take into account how often the numbers n and $n + k$ are simultaneously odd, as opposed to two randomly chosen integers. Moreover we need to do something similar with all primes p , or at least all the primes p up to some point. Thus the reasoning goes that $A_k(x) \sim \frac{x}{\log x}$ according to the prime number theorem, so $\pi_{\mathcal{A}_k}(x) \sim c_k \frac{x}{(\log x)^2}$ where

$$c_k = \lim_{q \rightarrow \infty} \frac{\frac{1}{x} \#\{n \leq x : (n(n+k), q) = 1\}}{(\frac{1}{x} \#\{m \leq x : (m, q) = 1\})^2}$$

and the limit over q -values occurs so that we take account of any peculiarities due to small primes; in particular, we want each fixed prime p to divide every sufficiently large q in the sequence. We observe that $c_k = 0$ if k is odd, due to the fact that $(n(n+k), 2) \neq 1$ for every integer n .

The usual choice for q -values are of the form $q = \prod_{p \leq y} p$, letting $y = y(x) \rightarrow \infty$.

How about integers missing digits? Suppose that $\mathcal{A}$ is the set of integers containing only the digits from the set $\mathcal{D} \subsetneq \{0, \dots, b-1\}$ in base b with $0 \in \mathcal{D}$. Up to $x = b^k$ there are $|\mathcal{D}|^k = x^{1-\delta}$ such integers where $\delta = \frac{\log b/|\mathcal{D}|}{\log b}$. Looking between b^k and b^{k+1} we deduce that $A(x) \asymp x^{1-\delta}$.⁴ Now the only moduli in which these are not equidistributed in the arithmetic progressions are those which share prime factors with b . Therefore we guess that $\pi_{\mathcal{A}}(x) \sim c_{\mathcal{A}} \frac{A(x)}{\log x}$ where $c_{\mathcal{A}} = \#\{d \in \mathcal{D} : (d, b) = 1\}/|\mathcal{D}|$. In fact, Maynard [10] has proved this provided $\mathcal{D}$ is fairly dense within $\{0, \dots, b-1\}$.

5.3. Evaluating the Constants

The ratios for c_k are easily calculated because, using the Chinese Remainder Theorem, we have

$$\frac{\frac{1}{x} \#\{n \leq x : (n(n+k), q) = 1\}}{(\frac{1}{x} \#\{m \leq x : (m, q) = 1\})^2} = \prod_{p|q} \frac{\frac{1}{x} \#\{n \leq x : (n(n+k), p) = 1\}}{(\frac{1}{x} \#\{m \leq x : (m, p) = 1\})^2}$$

and so the p th ratio is $(1 - \frac{\omega(p)}{p})/(1 - \frac{1}{p})^2$ where $\omega(p) = \#\{n \leq x : p \mid n(n+k)\}$ so that $\omega(p) = 2$, unless $p \mid k$ in which case $\omega(p) = 1$. Thus in this formulation

$$c_k = \lim_{y \rightarrow \infty} \prod_{p \leq y} \frac{(1 - \frac{\omega(p)}{p})}{(1 - \frac{1}{p})^2} \quad (1)$$

⁴ $\lim_{x \rightarrow \infty} A(x)/x^{1-\delta}$ does not exist, since if $d \notin \mathcal{D}$ then $A((d+1) \cdot b^k - 1) = A(d \cdot b^k - 1)$.

and one can prove that this limit exists, taking the primes in ascending order. One can see that the data for twin primes, given in Table 4, confirms this prediction, where $\text{Li}_2(x) := \int_2^x \frac{dt}{(\log t)^2}$.

x	$\pi_2(x) = \#\{\text{Primes } p, p+2 \leq x\}$	Error: $C_2 \text{Li}_2(x) - \pi_2(x)$
10^6	8169	79
10^7	58980	-226
10^8	440312	56
10^9	3424506	802
10^{10}	27412679	-1262
10^{11}	224376048	-7183
10^{12}	1870585220	-25353
10^{13}	15834664872	-66567
10^{14}	135780321665	-56771
10^{15}	1177209242304	-750443
10^{16}	10304195697298	-3142802
10^{17}	90948839353159	-6092169
10^{18}	808675888577436	12916170

Table 4: The number of twin primes, and the error in our prediction.

Our heuristic generalizes to all sorts of questions involving prime values of polynomials. For example let $\mathcal{A} = \{n^2 + 1 : n \in \mathbb{Z}\}$. Then $\omega(p) = 1 + (\frac{-4}{p})$, which equals 0 for half the primes (those $\equiv 3 \pmod{4}$) and 2 for half the primes (those $\equiv 1 \pmod{4}$). This means that the order in which you take the product in (1) really matters because the infinite product is not absolutely convergent.

So why do we order the primes in ascending order (and thus the q_y in a corresponding order)? Although this is not fundamentally suggested by our heuristic, it is by the circle method approach of Hardy and Littlewood (which is too involved to explain here) and calculations have shown that this ordering of the primes seems to be correct. My guess is that the underlying reason is that the period of $\{f(n) \pmod{p} : n = 1, 2, \dots\}$ is p , and we are ordering the primes so that the lengths of the periods appear in ascending order. This interpretation becomes important when trying to guess at the number of prime values in sequences like $\{k \cdot 2^n + 1\}_{n \geq 1}$.

6. Are There More than 52 Mersenne Primes?

If we assume that numbers of the form $2^n - 1$ are prime as often as regular integers of the same size then, by Gauss's heuristic, we would guess that

$$\#\{n \leq x : 2^n - 1 \text{ is prime}\} \approx \sum_{n \leq x} \frac{1}{\log(2^n - 1)} \sim \sum_{n \leq x} \frac{1}{n \log 2} \sim \frac{\log x}{\log 2}.$$

However, we established that if $2^n - 1$ is prime then $n = p$ is prime and so we should adjust this to

$$\#\{n \leq x : 2^n - 1 \text{ is prime}\} \approx \sum_{p \leq x} \frac{1}{\log(2^p - 1)} \sim \sum_{p \leq x} \frac{1}{p \log 2} \sim \frac{\log \log x}{\log 2},$$

which is a very different rate of growth though the first guess grows more like the small amount of data that we do have.

So far we have not taken into account divisibility by small primes. How we approached this above makes no sense since the integers $\{2^p - 1 : p \text{ prime}\}$ are pairwise coprime, and thus no prime divides more than one of them. We therefore look more carefully at what primes can possibly divide a particular $2^p - 1$ with prime p large. Now if prime q divides $2^p - 1$ then $\text{ord}_q(2) = p$ which must divide $q - 1$ by Fermat's Little Theorem, and so $q \equiv 1 \pmod{p}$. In particular none of the primes $\leq 2p$ can divide $2^p - 1$ if $p > 2$. Pomerance suggested modifying the above heuristic by a factor that takes account of this: That is, the proportion of integers near $x = 2^p - 1$ which are coprime to $m = \prod_{q \leq 2p} q$ that are prime is

$$\frac{1/\log x}{\frac{\phi(m)}{m}} \sim \frac{e^\gamma \log p}{p \log 2}$$

and so we guess that

$$\#\{n \leq x : 2^n - 1 \text{ is prime}\} \approx \sum_{p \leq x} \frac{e^\gamma \log p}{p \log 2} \sim \frac{e^\gamma}{\log 2} \log x.$$

This is compatible with the known data (see Table 5)

x	10^2	10^3	10^4	10^5	10^6	10^7	10^8
$2^p - 1$ prime, $p \leq x$	10	14	22	28	33	38	51
$e^\gamma \log_2 x$	12	18	24	29.5	35.5	41.5	47.5

Table 5: The number of Mersenne primes vs. our prediction

The predictions are an excellent fit with the data in Table 5, though one can criticise the heuristic since it only takes account of the primes $\leq 2p$. If say we try to extend this to divisibility by the primes $\leq p^2$ then $2^p - 1$ can only be divisible by the primes of the form $mp + 1$ of those $\leq p^2$, but it far from clear what factor to use for these primes in our product over primes.

6.1. Fibonacci Primes

If we apply Pomerance's heuristic to prime Fibonacci numbers (and recall that if F_n is prime and $n > 4$ then n is prime) then we guess that

$$\#\{n \leq x : F_n \text{ is prime}\} \sim \frac{e^\gamma}{\log \phi} \log x \text{ with } \phi := \frac{\sqrt{5} + 1}{2}.$$

This heuristic also seems compatible with the known data, as we see in Table 6.

x	10^2	10^3	10^4	10^5	10^6	$\frac{1}{3} \cdot 10^7$
F_n prime, $n \leq x$	12	21	26	33	43	50
$e^\gamma \log_\phi x$	17	25.5	34	42.5	51	55.5

Table 6: The number of Fibonacci primes vs. our prediction

Mersenne numbers and Fibonacci numbers are each defined by second order linear recurrence sequences that are also division sequences (that is, u_m divides u_n whenever m divides n so that if u_n is prime and $n > n_0$ then n is prime). At the end of the last subsection we claimed that Pomerance’s heuristic is rather dubious, so it is good to test it out in other situations where one can make the same criticism. The heuristic can be adapted to other second order linear recurrences that are also division sequences (in particular, Lucas sequences) and in all cases that Grantham and I were able to test [5] it is very compatible with the data: In Table 7 we give for various sequences of the form $\frac{a^n - b^n}{a - b}$, the number of primes with $n \leq 10^6$, as compared to the prediction from Pomerance’s heuristic.

Sequence	# primes	Predictions
$2^n - 1$	33	35.5
$(3^n - 1)/2$	18	22.5
$3^n - 2^n$	26	
$4^n - 3^n$	24	
$(5^n - 1)/4$	17	15
$(5^n - 2^n)/3$	22	
$(5^n - 3^n)/2$	20	
$5^n - 4^n$	20	

Table 7: The number of primes of the form $\frac{a^n - b^n}{a - b}$ vs. our predictions

7. Primes of the Form $a \cdot 2^n + b$

What about primes in second order linear recurrence sequences that are not division sequences? We saw this is quite different; for example, in the case $3 \cdot 2^n - 1$ we have primes for $n = 1, 2, 3, 4, 6, 7, 11, 18, 34, 38, 43, 55, 64, 76, 94$. We proceeded in [5] much as we did in Section 5 to guess that

$$\#\{\text{Primes } a \cdot 2^n + b : n \leq x\} \approx \kappa_{a,b} \sum_{n \leq x} \frac{1}{\log(a \cdot 2^n + b)} \sim c_{a,b} \log x$$

with $c_{a,b} = \frac{\kappa_{a,b}}{\log 2}$ where $\kappa_{a,b}$ is a constant that depends on the mod q properties of $a \cdot 2^n + b$. That is,

$$\kappa_{a,b} = \lim_{q \rightarrow \infty} \frac{\frac{1}{x} \# \{n \leq x : (a \cdot 2^n + b, q) = 1\}}{\frac{1}{x} \# \{m \leq x : (m, q) = 1\}}$$

where q runs through an appropriate (to be selected) sequence of integers. When we looked at prime values of polynomials we were able to write this ratio as the product of analogous ratios for each of the prime factors of q , using the Chinese Remainder Theorem. However, we have no such property here, remembering our example

$$\begin{aligned} 5 \text{ divides } 3 \cdot 2^n - 1 & \text{ if and only if } n \equiv 1 \pmod{4} \\ 11 \text{ divides } 3 \cdot 2^n - 1 & \text{ if and only if } n \equiv 2 \pmod{10}. \end{aligned}$$

7.1. To Select the q 's

Let r_m be the product of the primes p for which $\text{ord}_p(2) = m$, and let $q_y = 2 \prod_{m \leq y} r_m$. Then we believe that

$$\kappa_{a,b} = \lim_{y \rightarrow \infty} \frac{\frac{1}{x} \# \{n \leq x : (a \cdot 2^n + b, q_y) = 1\}}{\frac{1}{x} \# \{m \leq x : (m, q_y) = 1\}}.$$

It is evident that $\kappa_{a,b} = 0$ if there is a covering system (once Q divides q_y).

The odd primes p are ordered by the size of $\text{ord}_p(2)$ which seems the most relevant data for appreciating how they effect the primality of $a \cdot 2^n + b$. In [5] we could calculate this quantity in practice up to about $y = 30$ and it seems plausible that it always converges to a positive constant if there is no covering system. We could again compare our prediction to data in Table 8.

x	10^2	10^3	10^4	10^5	10^6
$3 \cdot 2^n - 1$ prime, $n \leq x$	15	25	30	43	53
$2^n - 3$ prime, $n \leq x$	13	27	34	49	61
Prediction	23	34	46	57	69

Table 8: The number of primes of the form $a \cdot 2^n + b$ vs. our predictions

In Table 8 we looked only at data for the forms $3 \cdot 2^n - 1$ and $2^n - 3$ (where our prediction is about the same for each sequence). In Table 9 we give data comparing the number of primes of the form $a \cdot 2^n + b$ with $n \leq 10^6$ with our prediction $c_{a,b} \log 10^6$, for various a, b -values.

$a \cdot 2^n + b$	# Primes	Prediction
$2^n - 1$	33	35.5
$2^n - 3$	61	69
$3 \cdot 2^n - 1$	53	69
$2^n + 3$	52	
$3 \cdot 2^n + 1$	42	51
$2^n - 5$	48	
$5 \cdot 2^n - 1$	39	51
$2^n + 5$	17	
$5 \cdot 2^n + 1$	22	21
$2^n - 7$	12	
$7 \cdot 2^n - 1$	21	18
$2^n + 7$	54	
$7 \cdot 2^n + 1$	34	52
$3 \cdot 2^n - 5$	53	
$5 \cdot 2^n - 3$	67	64
$3 \cdot 2^n + 5$	78	
$5 \cdot 2^n + 3$	74	77

Table 9: More primes of the form $a \cdot 2^n + b$ vs. our predictions

Although the predictions in Table 9 are not a perfect match with the data, we feel that they correlate reasonably given the limitations on how far we can compute. For example, we predict about four times as many primes of the form $2^n - 3$ as of the form $2^n - 7$, and the data up to 10^6 yields $\Pi_{1,-3}(10^6) = 61$, roughly five times $\Pi_{1,-7}(10^6) = 12$.

8. Conjectures for Primes of the Form $|a^m - b^n|$

One easily finds that

$$\#\{m, n \geq 1 : |a^m - b^n| \leq x\} \sim \frac{(\log x)^2}{\log a \log b}.$$

Assume that there is no two-dimensional covering system for $a^m - b^n$. Applying only Gauss's heuristic (that is, without modifying for divisibility by small primes) we would guess that

$$\#\{m, n \geq 1 : |a^m - b^n| \text{ is prime and } a^m, b^n \leq x\} \sim \frac{2 \log x}{\log a \log b}.$$

This implies that $\#\{\text{Primes } |a^m - b^n| \in (a^{100(k-1)}, a^{100k}]\}$ should be roughly constant as k varies (and indeed one can draw the same conclusion if one multiplies

a, b	$k=1$	2	3	4	5	6	7	First guess
2, 3	417	411	459	433	409	438	446	546
3, 4	294	299	284	297	290	283	263	433
2, 5	249	271	244	234	244	245	275	311
4, 5	293	245	278	290	253	294	269	311
5, 6	271	282	253	283	306	282	261	419
2, 7	175	171	185	148	202	172	160	240

Table 10: The number of primes of the form $|a^m - b^n|$ vs. our predictions. (Here the k th column gives $\#\{\text{Primes } |a^m - b^n| \in (a^{100(k-1)}, a^{100k}]\}$.)

through by a constant which accounts for divisibility by small primes). The data [6], some given in Table 10, suggests that this is true.

If we now take account of divisibility of small primes in much the same way as above we predict that

$$\#\{|a^m - b^n| \leq x : |a^m - b^n| \text{ is prime}\} \sim C_{a,b} \log x$$

for some constant $C_{a,b} > 0$ that we determine in an analogous way. We compare this more sophisticated prediction with the same data in Table 11. Again, this is mostly an impressively good fit.

a, b	$k=1$	2	3	4	5	6	7	Mean	Prediction
2, 3	417	411	459	433	409	438	446	430	424
3, 4	294	299	284	297	290	283	263	287	305
2, 5	249	271	244	234	244	245	275	252	225
4, 5	293	245	278	290	253	294	269	275	224
5, 6	271	282	253	283	306	282	261	277	279
2, 7	175	171	185	148	202	172	160	173	169

Table 11: The number of primes of the form $|a^m - b^n|$ vs. our revised predictions. Here we compare the mean of the seven columns with our revised prediction.

9. Apéry Primes

The Apéry numbers, defined by

$$a_n = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2,$$

play an important part in Apéry's proof of the irrationality of $\zeta(3)$. The integers $a_1 = 5, a_2 = 73, a_{12}$ and a_{24} are primes and no others with $n < 2000$; we do not

know whether any other Apéry numbers are prime. They are of particular interest to us because their value mod p is given by their base- p digits as follows:⁵

$$a(n_0 + n_1p + \cdots + n_dp^d) \equiv a(n_0)a(n_1) \cdots a(n_d) \pmod{p}.$$

Ron Graham suggested that the base p digits of a given randomly selected integer should be independent for different primes. From there he reasoned that there should only be finitely many integers n for which $\binom{2n}{n}, 105 = 1$, as follows: By Lucas' theorem we know that if p does not divide $\binom{2n}{n}$ then the base p digits of n

are all $\leq \frac{p-1}{2}$, and so if p is an odd prime then $\#\{n \leq x : p \nmid \binom{2n}{n}\} \asymp x^{\frac{\log \frac{p+1}{2}}{\log p}}$. Therefore the probability that a $p \nmid \binom{2n}{n}$ for a randomly chosen $n \leq x$ is $\asymp x^{-\frac{\log 3/2}{\log 3}}$ for $p = 3$, $\asymp x^{-\frac{\log 5/3}{\log 5}}$ for $p = 5$ and $\asymp x^{-\frac{\log 7/4}{\log 7}}$ for $p = 7$. Graham argued that since $\frac{\log 3/2}{\log 3} + \frac{\log 5/3}{\log 5} + \frac{\log 7/4}{\log 7} > 1$, thus $\binom{2n}{n}, 3 \cdot 5 \cdot 7 = 1$ for only finitely n .⁶

It seems reasonable to apply Graham's idea to Apéry numbers. Now $5 \mid a(m)$ for $m = 1$ and 3 so if n has a 1 or 3 in its base 5 expansion then $5 \mid a(n)$. Thus

$$\#\{n \leq x : a(n) \text{ is prime}\} \leq 1 + \#\{n \leq x : 5 \nmid a(n)\} \asymp x^{\frac{\log 3}{\log 5}}$$

since there are only 3 digits in base 5 with $a(n) \not\equiv 0 \pmod{5}$. More generally let $n_p := \#\{n \in [0, p-1] : p \mid a(n)\}$ (so $n_5 = 2$) so that

$$\#\{n \leq x : p \nmid a(n)\} \asymp x^{\frac{\log(p-n_p)}{\log p}} = x^{1-\sigma_p}$$

where $\sigma_p := -\frac{\log(1-n_p/p)}{\log p}$. Ron Graham's heuristic suggests that if $\sigma_Q := \sum_{p \mid Q} \sigma_p > 1$ then $(a(n), Q) > 1$ for all sufficiently large n . It is evident that there exists such an integer Q if and only if $\sum_p \sigma_p > 1$ where the sum is over all primes p .

The non-zero values of σ_p with $p < 100$ are $\sigma_{11} = 1, \sigma_5 = \sigma_{17} = \sigma_{19} = \sigma_{31} = \sigma_{37} = \sigma_{41} = \sigma_{59} = \sigma_{61} = \sigma_{73} = \sigma_{97} = 2$.⁷ Now $\sigma_{Q_{10}} = 0.31739 \cdots, \sigma_{Q_{10^2}} = 0.51496 \cdots, \sigma_{Q_{10^3}} = 0.58074 \cdots, \sigma_{Q_{10^4}} = 0.61336 \cdots$ where $Q_y = \prod_{p \leq y} p$. One gets the impression this converges to a constant $\sigma_\infty < 1$, so it seems unlikely that there is an integer Q with $\sigma_Q > 1$.

One can show that $a(n) \approx n^{O(1)}c^n$ where $c = (\sqrt{2} + 1)^4$, so the "probability" that a number near $a(n)$ is prime is $\sim 1/n \log c$. Taking into account divisibility by

⁵This type of property is familiar from Lucas' theorem which states that if $n = m + r$ then

$$\binom{n}{m} \equiv \binom{n_0}{m_0} \binom{n_1}{m_1} \cdots \binom{n_d}{m_d} \pmod{p}$$

where $n = n_0 + n_1p + \cdots + n_dp^d$, etc.

⁶That is, there are only finitely many integers whose digits in base 3 are only 0 and 1 , in base 5 are only $0, 1$ and 2 , and in base 7 are only $0, 1, 2$, and 3 .

⁷One observes that $a_n \equiv a_{p-1-n} \pmod{p}$ so n_p is even, unless $a_{\frac{p-1}{2}} \equiv 0 \pmod{p}$ which only happens very rarely (indeed only for $p = 11$ with $p < 10^4$).

5 we guess that the number of prime $a(n)$ values with $n \geq x$ is

$$\#\{n \leq x : a(n) \text{ is prime}\} \asymp \sum_{n \leq x} \frac{\text{Prob}(5 \nmid a(n) : n \leq x)}{n} \approx \sum_{n \leq x} \frac{1}{n^{1+\sigma_5}} < \infty$$

so we believe there are only finitely many Apéry primes.

Acknowledgements. This article is based on my presentation at the conference in honour of Nathanson and Pomerance. Thanks to Michael Filaseta and Nathan Jones for gently correcting the historical blunders in my presentation at the meeting. Indeed most of Section 4 is based on an email I received after my talk from Filaseta. Section 9 on Apéry primes evolved from a conversation with Armin Straub for which I thank him.

References

- [1] T. Cochrane and G. Myerson, Covering congruences in higher dimensions, *Rocky Mountain J. Math.* **26** (1996), 77–81.
- [2] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer Verlag, New York, 2001.
- [3] P. Erdős, On integers of the form $2^k + p$ and some related problems, *Summa Brasil. Math.* **2** (1950), 113–123.
- [4] M. Filaseta, C. Finch, and M. Kozek, On powers associated with Sierpiński numbers, Riesel numbers and Pólya’s conjecture, *J. Number Theory* **128** (2008), 1916–1940.
- [5] J. Grantham and A. Granville, Fibonacci primes, primes of the form $2^n - 1$ and beyond, *J. Number Theory* **261** (2024), 190–219.
- [6] A. Granville and F. Pappalardi, Two dimensional covering systems and possible prime producing $a^m - b^n$, preprint (2025).
- [7] A. Granville and P. Pleasants, Aurefeullian factorization revisited, *Mathematics of Computation* **75** (2006), 497–508.
- [8] R.K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, New York, 2004.
- [9] A.S. Izotov, A note on Sierpiński numbers, *Fibonacci Quart.* **33** (1995), 206–207.
- [10] J. Maynard, Primes with restricted digits, *Invent. Math.* **217** (2019), 127–218.
- [11] M. B. Nathanson, Sums of finite sets of integers, *Amer. Math. Monthly* **79** (1972), 1010–1012.
- [12] M. B. Nathanson, *Additive Number Theory: The Classical Bases*, Graduate Texts in Mathematics 164, Springer, 1996.
- [13] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Mathematics 165, Springer, 1996.

- [14] Š. Porubský, and J. Schönheim, Covering systems of Paul Erdős. Past, present and future, in “Paul Erdős and his mathematics, I”, (Budapest, 1999), 581–627. *Bolyai Soc. Math. Stud.*, **11** János Bolyai Mathematical Society, Budapest, 2002.
- [15] H. Riesel, Några stora primtal, *Elementa* **39** (1956), 258–260.
- [16] N. P. Romanoff, Über einige Sätze der additiven Zahlentheorie, *Math. Ann.* **109** (1934), 668–678.
- [17] A. Schinzel, On primitive prime factors of $a^n - b^n$, *Proc. Cambridge Philos. Soc.* **58** (1962), 555–562.
- [18] W. Sierpiński, Sur un problème concernant les nombres $k \cdot 2^n + 1$, *Elem. Math.* **15** (1960), 73–74.