PATTERNS IN PRIMES

KEITH CONRAD

Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate. Leonhard Euler

1. Introduction

It has been known since the time of ancient Greece that there are infinitely many primes. There are many unsolved problems about patterns among the primes. Here are a few.

- Are there infinitely many prime pairs $p, p+2$? These are twin primes.
- Are there infinitely many primes of the form n^2+1? These have no name.
- Are there infinitely many primes of the form 2^n-1? These are Mersenne primes.

It is expected that the answer to all three questions is "Yes".

Roughly speaking, a sequence of integers is expected to contain prime values infinitely often except when it obviously can't. Making precise what "obviously can't" means depends on the pattern being studied. Consider the following examples.

- There are finitely many primes of the form n^2-1: since $n^2-1=(n+1)(n-1)$, n^2-1 is prime only when $n=2$. There is no obvious reason n^2+1 can't be prime infinitely often, so we conjecture that it is.
- There are finitely many prime pairs n and $n+1$: the only example is 2 and 3. There is no obvious reason n and $n+2$ can't both be prime infinitely often (twin primes), so we conjecture that it is.

In Section 2 we'll describe when a nonconstant polynomial $f(x)$ in $\mathbf{Z}[x]$ is expected to take prime values infinitely often, such as x^2+1. This will rely on ideas from algebra and modular arithmetic. Section 3 extends the ideas from Section 2 to simultaneous prime values of several polynomials in $\mathbf{Z}[x]$, which includes twin primes (x and $x+2$). In Section 4 we look at primes in exponential sequences.

2. Qualitative Prime Patterns for a Single Polynomial

Let $f(x)$ be a nonconstant polynomial with integer coefficients, such as $11x+6$ or x^2+1. A few conditions are necessary in order for $f(n)$ to be prime infinitely often when $n \in \mathbf{Z}^+$:

(i) The leading coefficient of $f(x)$ is positive, since the sign of $f(x)$ is the sign of its leading coefficient when x is large.

(ii) We can't factor $f(x)$ into lower-degree polynomials with integer coefficients: if $f(x)=g(x)h(x)$ where $\deg g < \deg f$ and $\deg h < \deg f$ then $g(x)$ and $h(x)$ are nonconstant, so the equations $g(x)=0,\pm 1$ and $h(x)=0,\pm 1$ have finitely many solutions in $\mathbf{Z}$ (or in $\mathbf{R}$). Then for all large n, the equation $f(n)=g(n)h(n)$ shows $f(n)$ is composite since the factors $g(n)$ and $h(n)$ are not 0 or ± 1.

(iii) The coefficients of $f(x)$ have gcd 1. For example, the coefficients of $4x^3 - 6x^2 + 10$ have gcd 2, so for all $n \in \mathbf{Z}$ the integer $f(n)$ is even and thus is composite when n is large enough that $f(n) \neq 0, \pm 2$.

These three conditions are all necessary if we want $f(n)$ to be prime infinitely often as n runs over $\mathbf{Z}^+$. But they are *not* sufficient in general.

Example 2.1. The polynomial $x^2 - x - 4$ satisfies (i), (ii), and (iii), but $n^2 - n - 4$ is not prime for $n \in \mathbf{Z}^+$ other than at $n = 3$ because it is *always even*. (The solutions to $n^2 - n - 4 = 2$ are $n = 3, -2$.)

Example 2.2. The polynomial $x^3 - x - 6$ satisfies (i), (ii), and (iii), but $n^3 - n - 6$ is not prime for $n \in \mathbf{Z}^+$ since it is *always a multiple of* 3 (check $n^3 - n - 6 \equiv 0 \mod 3$ when $n \equiv 0, 1, 2 \mod 3$) and it is not 3 for $n \in \mathbf{Z}^+$.

There is an additional requirement $f(x)$ must satisfy to be prime infinitely often on $\mathbf{Z}^+$:

(iv) For no prime p is $f(n) \equiv 0 \mod p$ for all $n \in \mathbf{Z}/(p)$. Equivalently, for each prime p there is an $n \in \mathbf{Z}/(p)$ such that $f(n) \not\equiv 0 \mod p$.

The polynomials $x^2 - x - 4$ and $x^3 - x - 6$ don't satisfy (iv): $x^2 - x - 4$ fails (iv) at $p = 2$ and $x^3 - x - 6$ fails (iv) at $p = 3$.

Why does (iv) have to be satisfied if $f(n)$ is prime for infinitely many n in $\mathbf{Z}^+$? Since $f(x)$ is nonconstant, for a prime number p the equation $f(x) = p$ has only finitely many solutions, so if $f(n)$ is prime infinitely often on $\mathbf{Z}^+$, there is an $n \in \mathbf{Z}^+$ such that $f(n)$ is prime and $f(n) \neq p$. Then $f(n) \not\equiv 0 \mod p$, so (iv) holds.

Condition (iv) was discovered by Bunyakovsky [1], so we'll call it the *Bunyakovsky condition*. It implies (iii), since if the coefficients of $f(x)$ have gcd divisible by a prime p then $f(n) \equiv 0 \mod p$ for all $n \in \mathbf{Z}$. It is more restrictive than (iii) since polynomials like $x^2 - x - 4$ and $x^3 - x - 6$ that satisfy (iii) don't satisfy (iv): $x^2 - x + 4$ is identically 0 on $\mathbf{Z}/(2)$ and $x^3 - x + 6$ is identically 0 on $\mathbf{Z}/(3)$. Bunyakovsky proposed the following conjecture in 1854.

Conjecture 2.3 (Bunyakovsky)**.** *A nonconstant polynomial $f(x)$ with integer coefficients is prime infinitely often on the positive integers if and only if $f(x)$ satisfies conditions (i), (ii), (iii), and (iv).*

We have already explained why all of (i) through (iv) are necessary for $f(n)$ to be a prime number for infinitely many n in $\mathbf{Z}^+$. (There is a slight redundancy, since we pointed out that (iii) follows from (iv).) The point of Conjecture 2.3 is that it says the four conditions are also sufficient for $f(n)$ to have infinitely many prime values on $\mathbf{Z}^+$.

If $\deg f = 1$ then the Bunyakovsky condition automatically follows from (iii): writing $f(x) = a + mx$, condition (iii) for $a + mx$ means $(a, m) = 1$. Then $f(0) = a$ and $f(1) = a + m$ are relatively prime, so no prime p can be a factor of $f(0)$ and $f(1)$. A linear polynomial automatically satisfies condition (ii), and condition (i) says $m > 0$. Therefore Bunyakovsky's conjecture when $\deg f = 1$ says $a + mx$ is prime infinitely often when a and m are relatively prime and $m \in \mathbf{Z}^+$. The degree-one case of Bunyakovsky's conjecture was known before Bunyakovsky's work as the following theorem of Dirichlet from 1837.

Theorem 2.4 (Dirichlet)**.** *If a and m are relatively prime integers with $m \in \mathbf{Z}^+$ then there are infinitely many primes of the form $a + mn$ where $n \in \mathbf{Z}^+$.*

Here is a special case of Bunyakovsky's conjecture in degree 2.

Conjecture 2.5. *There are infinitely many primes of the form $n^2 + 1$.*

This conjecture goes back to Euler in 1752 [3, pp. 587–588], who computed numbers of the form n^2+1 and kept finding prime values arising. The primes of the form n^2+1 less than 10000 are 2, 5, 17, 37, 101, 197, 257, 401, 577, 677, 1297, 1601, 2917, 3137, 4357, 5477, 7057, 8101, and 8837. Euler at least implicitly asked whether there are infinitely many such primes. Conjecture 2.5 was included by Landau [5, p. 106] in his list of unsolved problems about primes at the 1912 International Congress of Mathematicians, so this is also called Landau's conjecture or Landau's problem.

Not only is Conjecture 2.5 still unproved, but *no* instance of Bunyakovsky's conjecture has been proved in degree greater than 1.

In practice it is easy to check that a polynomial in $\mathbf{Z}[x]$ satisfies condition (iii). To verify that a polynomial $f(x)$ satisfying condition (iii) also satisfies condition (iv), we only need to check (iv) at primes $p \leq \deg f$: for every prime p, $f(x) \bmod p$ is not the zero polynomial (its coefficients in $\mathbf{Z}$ are not all multiplies of p, by (iii)), and if $p > \deg f$ then $f(x) \bmod p$ is a polynomial of degree less than p, so it has less than p roots in $\mathbf{Z}/(p)$: therefore $f(n) \not\equiv 0 \bmod p$ for some $n \in \mathbf{Z}/(p)$. In order to confirm (iv) for the prime p, compute $f(n) \bmod p$ for $n = 0, 1, \ldots, p-1$ and see if we ever find a value that is nonzero mod p.

Example 2.6. If $f(x) = 3x^4 - x^3 - 5x + 6$ then (iii) is true since one of the coefficients is -1. To check if $f(x)$ satisfies (iv) it suffices to look at primes $p \leq 4$. For $p = 2$, $f(0) = 6 \equiv 0 \bmod 2$ and $f(1) = 3 \not\equiv 0 \bmod 2$. For $p = 3$, $f(0) = 6 \equiv 0 \bmod 3$, $f(1) = 3 \equiv 0 \bmod 3$, and $f(2) = 48 - 8 - 10 + 6 = 36 \equiv 0 \bmod 3$. Thus $f(x)$ fails condition (iv) at the prime 3. Concretely, this means $f(n)$ is always a multiple of 3: the initial values of $f(x)$ at positive integers are $3, 36, 207, 690, 1731, 3648, 6831, \ldots$.

Example 2.7. If $f(x) = 6x^4 + 10x + 15$ then (iii) is true since $(6, 10, 15) = 1$. To check if $f(x)$ satisfies (iv) it suffices to look at primes $p \leq 4$. For $p = 2$, $f(0) = 15 \not\equiv 0 \bmod 2$. For $p = 3$, $f(1) = 31 \not\equiv 0 \bmod 3$. So $f(x)$ satisfies (iv).

The last thing we need to explain in order to test Bunyakovsky's conjecture is how to check (ii): determine if $f(x)$ is or is not a product of two lower-degree polynomials in $\mathbf{Z}[x]$. If we can discover a factorization of $f(x)$ then there's nothing more to do, *e.g.*, if $f(x) = x^4+4$ and a little birdie or a computer tells you that $f(x) = (x^2 - 2x + 2)(x^2 + 2x + 2)$ then this is easy to verify afterwards, so (ii) fails for this $x^4 + 4$ (which means $n^4 + 4$ is composite for all large enough n, in fact for $n \geq 2$). But what about $f(x) = x^3 - 2$? A computer will tell you this is irreducible in $\mathbf{Z}[x]$, but how could you prove this on your own once you know which way it should go? We can use Bunyakovsky's conjecture as a guide: if (i), (iii), and (iv) have already been checked, then if (ii) were true Bunyakovsky's conjecture predicts $f(n)$ is prime infinitely often, and it turns out that if $f(n)$ is prime enough times then the following theorem tells us $f(x)$ doesn't factor into lower-degree parts!

Theorem 2.8. *If $f(x) \in \mathbf{Z}[x]$ has degree $d \geq 1$ and $|f(n)|$ is 1 or a prime number for $2d+1$ integers n then $f(x)$ is not a product of lower-degree polynomials in $\mathbf{Z}[x]$.*

Proof. Suppose $f(x) = g(x)h(x)$ in $\mathbf{Z}[x]$ where $\deg g < d$ and $\deg h < d$. Then $f(n) = g(n)h(n)$ for all integers n. If $|f(n)|$ is 1 or a prime number then $g(n) = \pm 1$ or $h(n) = \pm 1$. Since $g(x)$ takes on each value in $\mathbf{Z}$ at most $\deg g$ times and $h(x)$ takes on each value in $\mathbf{Z}$ at most $\deg h$ times, the number of integers n such that $g(n) = \pm 1$ or $h(n) = \pm 1$ is at most $2\deg g + 2\deg h = 2\deg f = 2d$. Therefore $|f(n)|$ can be 1 or a prime number at most $2d$ times, so if $|f(n)|$ is 1 or a prime number $2d+1$ times then we have a contradiction. $\square$

Example 2.9. Let $f(x) = x^3 - 2$. Then $2d + 1 = 7$ and $|f(n)|$ is 1 or a prime number at the 7 integers 0, 1, -1, -3, -5, 9, and 15.[1]

Example 2.10. Let $f(x) = 6x^4 + 10x + 15$. Then $2d + 1 = 9$ and $|f(n)|$ is a prime number at the 9 integers $n = 1, -1, 2, -4, -11, -13, 23$, and 29.

Theorem 2.8 can be applied to individual examples, but not to an infinite family of examples. For instance, results in abstract algebra imply that $x^d - 2$ doesn't factor into lower-degree polynomials in $\mathbf{Z}[x]$ for every $d \geq 1$, but you can't prove this using Theorem 2.8. If you don't understand why, go ahead and try.

3. Qualitative Prime Patterns for Several Polynomials

Let's now consider how often several polynomials can take on prime values at the same time. We start with the linear case. Since all primes other than 2 are odd, the difference between a pair of primes not including 2 has to be even. The following conjecture, which goes back to de Polignac [7] in 1849, says each even number occurs infinitely often as the difference between primes.

Conjecture 3.1 (de Polignac)**.** *For each positive even number c, there are infinitely many pairs of primes that differ by c. Equivalently, for each positive even number c there are infinitely many prime pairs p and $p + c$.*

This conjecture includes the infinitude of twin primes as a special case ($c = 2$). By work of Maynard, Tao, Zhang, and others announced during 2013 and 2014, it is known that Conjecture 3.1 is true for infinitely many even c, and also for some[2] even $c \leq 246$ [8], but it is not yet proved for any *specific* value of c. Before 2013 it had not been known that the gap between pairs of primes could be below any finite bound infinitely often (*e.g.*, infinitely many prime pairs differing by at most a billion).

Can there be infinitely many "triple primes" p, $p + 2$, and $p + 4$? They are all prime when $p = 3$, but that is it! Indeed, for each positive integer n at least one of the numbers $n, n+2, n+4$ is a multiple of 3, as shown in the table below (in each row the term 0 mod 3 occurs somewhere), so such a triple can't be all prime except when one of them is 3.

n mod 3	$n + 2$ mod 3	$n + 4$ mod 3
0	2	1
1	0	2
2	1	0

There is no obvious reason there can't be infinitely many prime triples of the form n, $n + 2$, and $n + 6$: the problem with $n, n + 2, n + 4$ does not occur for $n, n + 2, n + 6$ since, as the table below shows, none of them is a multiple of 3 when $n \equiv 2$ mod 3.

n mod 3	$n + 2$ mod 3	$n + 6$ mod 3
0	2	0
1	0	1
2	1	2

[1] If $\deg f = 2$ or 3 and $f(x)$ is a product of lower-degree polynomials in $\mathbf{Z}[x]$ then $f(x)$ has a linear factor and thus has a rational root. So another way of checking (ii) when $\deg f = 2$ or 3 is to show $f(x)$ has no rational root. This is inadequate in general if $\deg f \geq 4$ since a factorization into lower-degree polynomials is not guaranteed to have a factor of degree 1.

[2] More precisely, some even $c \leq 246$ is the gap between infinitely many pairs of *consecutive* primes.

For $n \leq 1000$, the triple $n, n+2, n+6$ is all prime for the following values of n:

$$5,\ 11,\ 17,\ 41,\ 101,\ 107,\ 191,\ 227,\ 311,\ 347,\ 461,\ 641,\ 821,\ 857,\ 881.$$

It is believed that there should be infinitely many prime triples $n, n+2, n+6$, but this problem lies deeper than the infinitude of twin primes since the first two terms in such a prime triple form a pair of twin primes.

Looking beyond pairs and triples of primes, when should a k-tuple of positive integers $n+h_1, n+h_2, \ldots, n+h_k$, for fixed $h_1, \ldots, h_k$ in $\mathbf{Z}$, all take prime values infinitely often as n runs over $\mathbf{Z}^+$? From what we discussed above, this is expected to be true for the pair $n, n+2$ and the triple $n, n+2, n+6$, and is not true for the triple $n, n+2, n+4$. It is believed that the only reason such a k-tuple should be prevented from having all prime values infinitely often is that there is a *divisibility obstruction*: there is a prime p such that, for all n in $\mathbf{Z}^+$, one of $n+h_1, n+h_2, \ldots, n+h_k$ is a multiple of p. For instance, n, $n+2$, or $n+4$ is a multiple of 3 for every n so there aren't infinitely many triple primes $n, n+2, n+4$.

Since the condition $n + h_i \equiv 0 \bmod p$ is the same as $n \equiv -h_i \bmod p$, the divisibility obstruction in the previous paragraph is the same as every positive integer being congruent to one of $-h_1, -h_2, \ldots, -h_k \bmod p$. The positive integers fill up $\mathbf{Z}/(p)$, as do the negative integers, so the obstruction here is equivalent to saying $\{h_1, h_2, \ldots, h_k \bmod p\} = \mathbf{Z}/(p)$, *e.g.*, $\{1, 2, 4 \bmod 3\} = \mathbf{Z}/(3)$. In particular, we only need to check for this obstruction at the primes $p \leq k$ since it automatically fails at larger primes: k integers don't fill up $\mathbf{Z}/(p)$ when $p > k$.

Example 3.2. The 6-tuple $n, n+2, n+6, n+8, n+12, n+14$ is not prime infinitely often. If we reduce the constant terms modulo 2, 3, and 5 (the primes up to 6), we see in the table below that that they fill up all values modulo 5. That means such a 6-tuple always contains a multiple of 5, so we don't get such prime 6-tuples for infinitely many n; in fact, the 6-tuple contains all prime values only once, when $n = 5$.

p	$0 \bmod p$	$2 \bmod p$	$6 \bmod p$	$8 \bmod p$	$12 \bmod p$	$14 \bmod p$
2	0	0	0	0	0	0
3	0	2	0	2	0	2
5	0	2	1	3	2	4

On the other hand, if we consider the 6-tuple $n, n+2, n+6, n+8, n+12, n+18$ then the table below shows the constant terms don't fill up $\mathbf{Z}/(p)$ for a prime $p \leq 6$, and this means we expect there to be infinitely many prime 6-tuples of this form.

p	$0 \bmod p$	$2 \bmod p$	$6 \bmod p$	$8 \bmod p$	$12 \bmod p$	$18 \bmod p$
2	0	0	0	0	0	0
3	0	2	0	2	0	0
5	0	2	1	3	2	3

For n up to 1,000,000, the 6-tuple $n, n+2, n+6, n+8, n+12, n+18$ is prime six times: when n is 5, 11, 1481, 165701, 326141, and 661091. (The gap from the 3rd to 4th example is striking, and nearly repeats itself from the 4th to 5th example.)

Conjecture 3.3 (Dickson)**.** *For $h_1, h_2, \ldots, h_k \in \mathbf{Z}$, infinitely many $n \in \mathbf{Z}^+$ make the k-tuples $n+h_1, n+h_2, \ldots, n+h_k$ all prime if no prime $p \leq k$ satisfies $\{h_1, \ldots, h_k \bmod p\} = \mathbf{Z}/(p)$.*

Conjecture 3.3 was first made by Dickson [2] in 1904.[3] The work of Maynard and Tao [6] implies that, for each k, Conjecture 3.3 is true for infinitely many $(h_1, \ldots, h_k)$, but it is not known for any explicit k-tuple when $k \geq 2$.

Let's now consider a finite set of nonconstant polynomials $f_1(x), \ldots, f_k(x)$ with integer coefficients. When should we expect there to be infinitely many $n \in \mathbf{Z}^+$ making $f_1(n), \ldots, f_k(n)$ all prime? If this is going to happen then each $f_i(x)$ has to have infinitely many prime values, so each $f_i(x)$ needs to satisfy the four conditions in Bunyakovsky's conjecture. But this is not enough.

Example 3.4. Let $f_1(x) = x^2 + 1$ and $f_2(x) = x^3 - 2$. Each polynomial separately satisfies the conditions of Bunyakovsky's conjecture, and numerical data (see checkmarks in the table below) suggest they separately are often prime, but it never happens at the same time (the checkmarks are never in the same column).

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
n^2+1	✓	✓		✓		✓				✓				✓		✓				✓
n^3-2									✓						✓				✓	

Indeed, for every positive integer n either $n^2 + 1$ or $n^3 - 2$ is even, as shown by the rows of the table below. Therefore $n^2 + 1$ can only be prime for even n other than $n = 1$ (the one $n \in \mathbf{Z}^+$ at which $n^2 + 1 = 2$) and $n^3 - 2$ can be prime only for odd n.

n mod 2	n^2+1 mod 2	n^3-2 mod 2
0	1	0
1	0	1

In order that $f_1(n), \ldots, f_k(n)$ are prime together infinitely often, we don't just need each $f_i(x)$ to satisfy the Bunyakovsky condition (iv), but we need the *product* $f_1(x) \cdots f_k(x)$ to satisfy (iv): for no prime p is $f_1(n) \cdots f_k(n) \equiv 0 \bmod p$ for all $n \in \mathbf{Z}/(p)$. For instance, this would avoid a situation as in the previous example, where $(n^2+1)(n^3-2)$ is even for all n.

The reason (iv) has to be satisfied by the product $f_1(x) \cdots f_k(x)$ is similar to the reason we gave earlier in the case of a single polynomial: since each $f_i(x)$ is nonconstant, for a prime p each equation $f_i(x) = p$ has finitely many solutions, so if all the $f_i(n)$ are simultaneously prime for infinitely many $n \in \mathbf{Z}^+$, there is an $n \in \mathbf{Z}^+$ such that all $f_i(n)$ are prime and not equal to p. That means $f_i(n) \not\equiv 0 \bmod p$ for $i = 1, \ldots, k$, so $f_1(n) \cdots f_k(n) \not\equiv 0 \bmod p$.

Conjecture 3.5 (Schinzel)**.** *If $f_1(x), \ldots, f_k(x)$ in $\mathbf{Z}[x]$ are nonconstant, each satisfies the first three conditions of Bunyakovsky's conjecture, and the product $f_1(x) \cdots f_k(x)$ satisfies the Bunyakovsky condition, then there are infinitely many $n \in \mathbf{Z}^+$ such that $f_1(n), \ldots, f_k(n)$ are all prime.*

Conjecture 3.5 is called Schinzel's "Hypothesis H" and goes back to 1958 [9]. It includes all previous conjectures we have listed as special cases.

Example 3.6. We show Conjecture 3.3 is a special case of Conjecture 3.5 for the polyomials $x+h_1, \ldots, x+h_k$. These polynomials each satisfy (i), (ii), and (iii). For $(x+h_1) \cdots (x+h_k)$ to satisfy the Bunyakovsky condition, for each prime p we need $(n+h_1) \cdots (n+h_k) \not\equiv 0 \bmod p$ for some $n \in \mathbf{Z}/(p)$. That is equivalent to saying there is an integer n such that $n \not\equiv$

[3] About 20 years later Hardy and Littlewood [4, p. 61] formulated a quantitative version of Conjecture 3.3, predicting about how many $n \leq x$ make the k-tuple all prime, as x grows. Therefore Conjecture 3.3 is often attributed to Hardy and Littlewood.

$-h_1, \ldots, -h_k \bmod p$, or in other words $\{h_1, \ldots, h_k \bmod p\} \neq \mathbf{Z}/(p)$. This is automatically true when $p > k$, and for $p \leq k$ this condition is precisely the hypothesis in Conjecture 3.3.

It can be shown that a product of polynomials in $\mathbf{Z}[x]$ that each satisfy (iii) also satisfies (iii),[4] so when $f_1(x), \ldots, f_k(x)$ all satisfy (iii) the product $f_1(x) \cdots f_k(x)$ satisfies the Bunyakovsky condition for all primes $p > \deg(f_1(x) \cdots f_k(x))$, and therefore the Bunyakovsky condition for $f_1(x) \cdots f_k(x)$ only has to be checked at the primes $p \leq \deg(f_1(x) \cdots f_k(x))$.

Example 3.7. It is left to the reader to check that $x^2 + 1$ and $x^3 - 5$ satisfy conditions (i), (ii), and (iii) in Bunyakovsky's conjecture (you could use Theorem 2.8 to check (ii) for them), and the product $f(x) = (x^2+1)(x^3-5)$ satisfies the Bunyakovsky condition at each prime $p \leq \deg f$:

$$f(0) = -5 \not\equiv 0 \bmod 2, \quad f(0) = -5 \not\equiv 0 \bmod 3, \quad f(1) = -8 \not\equiv 0 \bmod 5.$$

Therefore Schinzel's Hypothesis H predicts that $n^2 + 1$ and $n^3 - 5$ are both prime for infinitely many n, and with a computer they are both prime for the following n up to 1000: $2, 4, 6, 16, 66, 94, 126, 204, 406$, 444, 576, 636, 816, 906, and 966.

4. Exponential Prime Patterns

Switching from polynomial expressions to exponential expressions, let's consider numbers of the form $a^n - 1$ with $a \geq 2$ and $n \geq 2$. When could this be prime?

Theorem 4.1. *For integers $a \geq 2$ and $n \geq 2$, $a^n - 1$ can be prime only if $a = 2$ and n is prime.*

Proof. From the factorization

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1), \tag{4.1}$$

if $a \geq 3$ then the factors on the right are both greater than 1 (the first is at least 2 and the second is at least 4), so $a^n - 1$ is composite for all $n \geq 2$.

Suppose now that $a = 2$. If n is composite, say $n = k\ell$ where $k, \ell \geq 2$, then we have the factorization

$$2^n - 1 = 2^{k\ell} - 1 = (2^k)^\ell - 1 = (2^k - 1)((2^k)^{\ell-1} + (2^k)^{\ell-2} + \cdots + 2^k + 1),$$

where the first factor on the right is at least $2^2 - 1 = 3$ and the second factor is at least $2^2 + 1 \geq 5$. Therefore $2^n - 1$ is composite when n is composite. □

For small primes p, $2^p - 1$ is prime:

$$2^2 - 1 = 3, \quad 2^3 - 1 = 7, \quad 2^5 - 1 = 31, \quad 2^7 - 1 = 127.$$

However, $2^{11} - 1 = 23 \cdot 89$ and $2^{23} - 1 = 47 \cdot 178481$. Primes of the form $2^p - 1$ are called *Mersenne primes* after Marin Mersenne, a French priest who wrote about them in 1644. The first ten Mersenne primes $2^p - 1$ occur for $p = 2$, 3, 5, 7, 13, 17, 19, 31, 61, and 89.

Conjecture 4.2. *There are infinitely many Mersenne primes.*

[4] In abstract algebra the name for this is Gauss' lemma: a product of primitive polynomials in $\mathbf{Z}[x]$ is also primitive.

Because the numbers $2^n - 1$ grow so quickly (*e.g.*, the 20th Mersenne prime has over 1,000 digits), very few Mersenne primes are known. As of the time this is written, only 51 Mersenne primes have been found, with the largest being $2^p - 1$ for $p = 82{,}589{,}933$. This Mersenne prime was found in December 2018 and has over 24 million digits. There is currently a $150,000 prize for the first prime number (of any kind) found with over 100 million digits.

Let's switch the second term in $2^n - 1$ to $+1$ instead of -1: when is $2^n + 1$ prime? The necessary condition on n is something different from being prime.

Theorem 4.3. *For $n \geq 2$, $2^n + 1$ can be prime only if n is a power of 2.*

Proof. If n is odd then $2^n + 1$ is a multiple of 3: $2^n + 1 \equiv (-1)^n + 1 \equiv -1 + 1 \equiv 0 \bmod 3$. Therefore we can't have n be odd and greater than 1 if $2^n + 1$ is prime.

Suppose n is not necessarily odd but has an odd factor greater than 1: $n = MN$ where $N > 1$ is odd. (For example, $n = 12 = 4 \cdot 3$.) Then $2^n + 1 = (2^M)^N + 1$, which is divisible by $2^M + 1$ by the above reasoning with N in place of n and 2^M in place of 2. Therefore $2^n + 1$ can be prime only if n has no odd factor greater than 1, which means n has no odd prime factor, so n must be a power of 2.[5] □

Integers of the form $2^{2^m} + 1$ where $m \geq 0$ are called *Fermat numbers*, since Fermat observed in the 1600s that $2^{2^m} + 1$ is prime when $m = 0, 1, 2, 3, 4$ and he conjectured that $2^{2^m} + 1$ is prime for all larger m. Its value at $m = 5$ is

$$2^{2^5} + 1 = 4294967297,$$

and Euler found a nontrivial factorization of this in 1732, so Fermat was wrong:

$$2^{2^5} + 1 = 641 \cdot 6700417.$$

No further prime values of $2^{2^m} + 1$ have been found, and it is now believed that Fermat was completely wrong:

Conjecture 4.4. *For $m \geq 5$, $2^{2^m} + 1$ is composite.*

Factoring numbers of the form $2^{2^m} + 1$ is very difficult because of their rapid growth. For example, $2^{2^{20}} + 1$ was proved to be composite indirectly in 1987, but no explicit nontrivial factor of this number is known.

If we look at numbers $k \cdot 2^n - 1$ where $k > 1$ is odd, primality does not require n to be prime anymore. For example, $7 \cdot 2^{45} - 1$ is prime. Changing -1 to $+1$, numbers of the form $k \cdot 2^n + 1$ for odd $k > 1$ can mimic the behavior of $2^n + 1$, which appears to be so rarely prime: for some odd $k > 1$, $k \cdot 2^n + 1$ is composite for *all* $n \geq 1$. For example, $78557 \cdot 2^n + 1$ is composite for all $n \geq 1$. It is conjectured that 78557 is the smallest odd number with that property; this is called the Sierpinski problem.

Appendix A. The logic behind Dirichlet's theorem

Dirichlet's theorem says there are infinitely many primes satisfying $p \equiv a \bmod m$ when $(a, m) = 1$. You might think it might be easier to show there is at least one prime $p \equiv a \bmod m$ whenever $(a, m) = 1$, but that turns out to be just as hard as Dirichlet's theorem!

Theorem A.1. *The following two statements are equivalent.*

[5] By similar reasoning, if a is a positive integer greater than 1 and $a^n + 1$ is prime with $n > 1$ then n is a power of 2.

(1) *For all positive integers a and m such that $(a, m) = 1$, there is a prime $p \equiv a \bmod m$.*
(2) *For all positive integers a and m such that $(a, m) = 1$, there are infinitely many primes $p \equiv a \bmod m$.*

This is very surprising. The theorem seems to be saying, for instance, that by knowing there is one prime $p \equiv 4 \bmod 7$, like $p = 11$, it follows that there are infinitely many primes $p \equiv 4 \bmod 7$. But it doesn't say anything like that. The role of quantifiers in Theorem A.1 is critical: the two equivalent statements in the theorem are each running over *all* pairs of relatively prime positive integers. Neither statement is about a single case of a and m. When you read the proof of the theorem just below you'll see this aspect of the underlying logic is essential for the proof to work.

Proof. We will show the first statement in Theorem A.1 implies the second statement; the other direction is trivial.

Pick positive integers a and m with $(a, m) = 1$. By hypothesis there is a prime $p_1 \equiv a \bmod m$. We want to show there are infinitely many primes $p \equiv a \bmod m$. We can suppose $m > 1$ since what we want to show is obvious if $m = 1$: all integers are congruent to each other modulo 1 and we know there are infinitely many primes.

Since the congruence condition "$p \equiv a \bmod m$" doesn't change if we adjust a modulo m, there is no harm in supposing $0 < a < m$. (For example, instead of looking at the condition $p \equiv 8 \bmod 5$, look at it as $p \equiv 3 \bmod 5$; that's the same thing.)

Assume we have r different primes $p_1, p_2, \ldots, p_r$ that all satisfy $p_i \equiv a \bmod m$. We want to find an additional such prime. Then, since r was arbitrary, that means the set of primes $p \equiv a \bmod m$ is infinite.

We will find a prime $p \equiv a \bmod m$ that is not any of the p_i by using the first statement of Theorem A.1 with a *different* choice of a and m.

Since $m > 1$, its powers eventually exceed every p_i: let $m^k > p_1, \ldots, p_r$. Now consider the congruence condition

$$p \equiv a + m^k \bmod m^{k+1}. \tag{A.1}$$

Here we are replacing a with $a + m^k$ and the modulus m with a new modulus m^{k+1}. The numbers $a + m^k$ and m^{k+1} are relatively prime since a and m are relatively prime (why?). Thus, by the first statement in Theorem A.1 with this new choice of "a" and "m" there is a prime p that satisfies (A.1). By reducing both sides of (A.1) modulo m, which we can do since m is a factor of m^{k+1}, we get $p \equiv a \bmod m$. It remains to show p is not any of $p_1, p_2, \ldots, p_r$.

Since $0 < a < m$, we have

$$0 < a + m^k < m + m^k \leq m^{k+1},$$

so $a + m^k$ is a standard remainder modulo m^{k+1}. Thus the (positive!) prime p satisfying (A.1) must be at least $a + m^k$. (This would no longer be true in general if we didn't have $0 < a + m^k < m^{k+1}$, *e.g.*, not all primes $p \equiv 8 \bmod 5$ must be at least 8 – try $p = 3$.) Combining the inequalities $p_i < m^k < a + m^k$ with $p \geq a + m^k$ we get $p_i < p$ for $i = 1, \ldots, r$, so p is not any p_i. □

Theorem A.1 tells us that it is just as hard to show there is one prime number $p \equiv a \bmod m$ *whenever* $(a, m) = 1$ as it is to show there are infinitely many such prime numbers. While for concrete choices of relatively prime a and m we can generally find a prime $p \equiv$

$a \bmod m$ by computation, the only known way to prove there is a prime $p \equiv a \bmod m$ *whenever* $(a, m) = 1$ is to prove there are infinitely many such primes.

There is an analogue of Theorem A.1 for higher-degree polynomials in the setting of Bunyakovsky's conjecture, as follows.

Theorem A.2. *The following conditions are equivalent.*

(1) *For all nonconstant* $f(x) \in \mathbf{Z}[x]$ *that satisfy all the conditions of Bunyakovsky's conjecture,* $f(n)$ *is prime for some* $n \in \mathbf{Z}^+$.
(2) *For all nonconstant* $f(x) \in \mathbf{Z}[x]$ *that satisfy all the conditions of Bunyakovsky's conjecture,* $f(n)$ *is prime for infinitely many* $n \in \mathbf{Z}^+$.

Proof. Trivially (2) implies (1). For a proof that (1) implies (2), see https://mathoverflow.net/questions/226794. □

An analogue of Theorem A.2 carries over to Schinzel's Hypothesis H: if every set of nonconstant polynomials in $\mathbf{Z}[x]$ that fit the conditions of Hypothesis H has simultaneous prime values for at least one positive integer then every set of nonconstant polynomials in $\mathbf{Z}[x]$ that fit the conditions of Hypothesis H has simultaneous prime values for infinitely many positive integers.

References

[1] V. Bouniakowsky, "Sur les diviseurs numériques invariables des fonctions rationnelles entières," *Mémoires sc. math. et phys.* **6** (1854), 306–329.
[2] L. E. Dickson, L. E. "A new extension of Dirichlet's theorem on prime numbers," *Messenger of Mathematics* **33** (1904), 155–161.
[3] L. Euler, Letter 149 to Goldbach Oct. 28, 1752, pp. 586–591 in *Corr. Math. et Physique* Tome I, St. Petersburg, 1843. Online at https://archive.org/details/correspondancem01goldgoog/page/n753.
[4] G. H. Hardy and J. E. Littlewood, "Some problems of 'Partitio numerorum' III: on the expression of a number as a sum of primes," *Acta Math.* **44** (1923), 1–70. Online at https://projecteuclid.org/euclid.acta/1485887559.
[5] E. Landau, Gelöste und ungelöste Probleme aus der Theorie der Primzahlverteilung und der Riemannschen Zetafunktion, pp. 93–108 in "Proceedings of the Fifth International Congress of Mathematicians, I" Cambridge Univ. Press, London, 1913. Online at https://www.mathunion.org/fileadmin/ICM/Proceedings/ICM1912.1/ICM1912.1.ocr.pdf.
[6] J. Maynard, "Small gaps between primes," *Annals of Math.* **181** (2015), 383–413.
[7] A. de Polignac, "Recherches nouvelles sur les nombres premiers," *Comptes Rendus des Séances de l'Académie des Sciences* **29** (1849), 397-401, Erratum, 738–739.
[8] D. H. J. Polymath, "Variants of the Selberg sieve, and bounded intervals containing many primes," *Research in the Mathematical Sciences* **1** (2014), 83 pages.
[9] A. Schinzel and W. Sierpinski, "Sur certaines hypothèses concernant les nombres premiers," *Acta Arith.* **4** (1958), 185–208, Erratum **5** (1959), 259.