1. Introduction

Numerical data suggest the following patterns for prime numbers $p$:

- $-1 \equiv \square \mod p \iff p = 2$ or $p \equiv 1 \mod 4$,
- $2 \equiv \square \mod p \iff p = 2$ or $p \equiv 1, 7 \mod 8$,
- $-2 \equiv \square \mod p \iff p = 2$ or $p \equiv 1, 3 \mod 8$,
- $3 \equiv \square \mod p \iff p = 2, 3$ or $p \equiv 1, 11 \mod 12$,
- $-3 \equiv \square \mod p \iff p = 2, 3$ or $p \equiv 1 \mod 3$,
- $5 \equiv \square \mod p \iff p = 2, 5$ or $p \equiv 1, 4 \mod 5$.

As an application of such equivalences, we will use them to prove there are infinitely many primes in certain arithmetic progressions by adapting a proof going back to Euclid that there are infinitely many primes.

2. Euclid’s Proof of the Infinitude of the Primes

Euclid’s *Elements*, which is famous mostly for its rigorous development of the theorems of plane geometry from five axioms, contains a fair bit of number theory: the Euclidean algorithm gets its name from its appearance in this work, and the existence of prime factorization is proved here as well. Proposition 20 of Book IX of the Elements proves the infinitude of the set of prime numbers. Here is that argument, in modern language.

**Theorem 2.1** (Euclid). There are infinitely many prime numbers.

**Proof.** We know some primes already, such as 2. (We could list some more, but we just need one of them.) Suppose $p_1, \ldots, p_r$ are all prime. We want to show there is another prime off this list. The key idea is to consider the number

$$N = p_1 \cdots p_r + 1.$$  

That is the product of all the primes in the list, plus one. The number $N$ is not divisible by any of $p_1, \ldots, p_r$ since $N$ has remainder 1 when divided by each $p_i$. Since $N > 1$, $N$ has a prime factor, say $p$. This prime is different from $p_1, \ldots, p_r$ since $N$ is divisible by $p$ but not by any $p_i$.

If there were finitely many primes, then running through the above argument with $p_1, \ldots, p_r$ being the complete list of primes shows there is another prime, which is a contradiction. Therefore there are infinitely many primes. \qed

A common misunderstanding of this proof is that it is saying if $p_1, \ldots, p_r$ are all prime then $p_1 \cdots p_r + 1$ is prime. *This need not be true.* For example, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 20031 = 59 \cdot 509$. What the proof says is that if $p_1, \ldots, p_r$ are all prime then any prime factor of $p_1 \cdots p_r + 1$ will be a prime other than one of the $p_i$’s, but not that $p_1 \cdots p_r + 1$ is itself prime.
Remark 2.2. Here is a recursive way to find new primes, suggested by Euclid’s proof: set $p_1 = 2$, and if we have primes $p_1, \ldots, p_r$ then let $p_{r+1}$ be the smallest prime factor of $p_1 p_2 \cdots p_r + 1$. For instance, $p_1 + 1 = 3$ is prime, so $p_2 = 3$, and $p_1 p_2 + 1 = 7$ is prime, so $p_3 = 7$. This list of primes falls out in the following order:

\[
2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, \ldots
\]

Does this list eventually include all primes? Nobody knows.

3. Extending Euclid’s proof to primes in arithmetic progression

An arithmetic progression is a sequence with a common difference between successive terms. It has the form $a, a + m, a + 2m, a + 3m, a + 4m, \ldots$. For example, the (positive) odd numbers are an arithmetic progression with $a = 1$ and $m = 2$. We will focus on arithmetic progressions where $0 < a < m$. In the language of congruences, an arithmetic progression is the set of (positive) integers $n$ satisfying a congruence condition $n \equiv a \mod m$.

If $(a, m) > 1$ then the arithmetic progression $a, a + m, a + 2m, a + 3m, a + 4m, \ldots$ contains at most one prime number since every term in this arithmetic progression is a multiple of $(a, m)$. For example, there is only one prime $p \equiv 2 \mod 4$ and there are no primes $p \equiv 6 \mod 8$. If $(a, m) = 1$, on the other hand, there is no obvious reason there couldn’t be infinitely many primes $p \equiv a \mod m$, and Dirichlet proved there really are infinitely many such primes.

**Theorem 3.1** (Dirichlet, 1837). If $(a, m) = 1$ then there are infinitely many prime numbers $p \equiv a \mod m$.

The proof of Dirichlet’s theorem in general is hard, but special cases are accessible to the strategy of Euclid’s proof that there are infinitely many primes. We will show for the $a$ and $m$ in the table below that there are infinitely many primes $p \equiv a \mod m$. Most of the proofs in Section 3 will use the square patterns in the introduction.

<table>
<thead>
<tr>
<th>$a \mod m$</th>
<th>Theorem</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 mod 3</td>
<td>3.2</td>
</tr>
<tr>
<td>2 mod 3</td>
<td>3.3</td>
</tr>
<tr>
<td>1 mod 4</td>
<td>3.4</td>
</tr>
<tr>
<td>3 mod 4</td>
<td>3.5</td>
</tr>
<tr>
<td>4 mod 5</td>
<td>3.6</td>
</tr>
<tr>
<td>3 mod 8</td>
<td>3.7</td>
</tr>
<tr>
<td>5 mod 8</td>
<td>3.8</td>
</tr>
<tr>
<td>7 mod 8</td>
<td>3.9</td>
</tr>
<tr>
<td>5 mod 12</td>
<td>3.10</td>
</tr>
<tr>
<td>7 mod 12</td>
<td>3.11</td>
</tr>
<tr>
<td>11 mod 12</td>
<td>3.12</td>
</tr>
</tbody>
</table>

**Theorem 3.2.** There are infinitely many primes $p \equiv 1 \mod 3$.

**Proof.** One such prime is 7. If $p_1, \ldots, p_r$ are primes $\equiv 1 \mod 3$, let

\[
N = (2p_1 p_2 \cdots p_r)^2 + 3.
\]

Then $N$ is not divisible by 2, 3, or by any of $p_1, \ldots, p_r$ (why?). Since $N > 1$, $N$ has a prime factor, say $p$. Writing the condition $N \equiv 0 \mod p$ as $(2p_1 \cdots p_r)^2 + 3 \equiv 0 \mod p$, we have $-3 \equiv (2p_1 \cdots p_r)^2 \mod p$, so $-3 \equiv \square \mod p$. Therefore, since $p \neq 2$ or 3, the pattern
for $-3 \equiv \square \mod p$ tells us $p \equiv 1 \mod 3$. This prime is different from $p_1, \ldots, p_r$, since $N \equiv 3 \not\equiv 0 \mod p_i$ while $N \equiv 0 \mod p$, so there are infinitely many primes $\equiv 1 \mod 3$. \hfill \square

Theorem 3.3. There are infinitely many primes $p \equiv 3 \mod 4$.

**Proof.** One such prime is 2. If $p_1, \ldots, p_r$ are primes $\equiv 2 \mod 3$, let

$$N = 3p_1p_2 \cdots p_r - 1.$$  

Then $N$ is not divisible by 3 or by any of $p_1, \ldots, p_r$. Since $N > 1$, $N$ has a prime factor. Since $N \equiv -1 \equiv 2 \mod 3$, the prime factors of $N$ are not all $1 \mod 3$; otherwise $N \equiv 1 \mod 3$, because an integer greater than 1 is the product of its primes factors to some powers. Therefore $N$ has a prime factor $p$ that is $\equiv 2 \mod 3$. This prime is different from $p_1, \ldots, p_r$, since $N \equiv -1 \not\equiv 0 \mod p_i$ while $N \equiv 0 \mod p$, so there are infinitely many primes $\equiv 2 \mod 3$. \hfill \square

Theorem 3.4. There are infinitely many primes $p \equiv 1 \mod 4$.

**Proof.** One such prime is 5. If $p_1, \ldots, p_r$ are primes $\equiv 1 \mod 4$, let

$$N = (2p_1p_2 \cdots p_r)^2 + 1.$$  

Then $N$ is not divisible by 2 or by any of $p_1, \ldots, p_r$. Since $N > 1$, $N$ has a prime factor, say $p$. Then the condition $N \equiv 0 \mod p$ implies $-1 \equiv \square \mod p$ (why?). Since $p \not\equiv 2$, the pattern for $-1 \equiv \square \mod p$ tells us $p \equiv 1 \mod 4$. This prime is different from $p_1, \ldots, p_r$, since $N \equiv 1 \not\equiv 0 \mod p_i$ while $N \equiv 0 \mod p$, so there are infinitely many primes $\equiv 1 \mod 4$. \hfill \square

Theorem 3.5. There are infinitely many primes $p \equiv 3 \mod 4$.

**Proof.** One such prime is 3. If $p_1, \ldots, p_r$ are primes $\equiv 3 \mod 4$, let

$$N = 4p_1p_2 \cdots p_r - 1 > 1.$$  

Then $N$ is not divisible by 2 or by any of $p_1, \ldots, p_r$. Since $N \equiv -1 \equiv 3 \mod 4$, the prime factors of $N$ are not all $1 \mod 4$ (otherwise $N \equiv 1 \mod 4$). Therefore $N$ has a prime factor $p$ that is $3 \mod 4$. This prime is different from $p_1, \ldots, p_r$, since $N \equiv -1 \not\equiv 0 \mod p_i$ while $N \equiv 0 \mod p$, so there are infinitely many primes $\equiv 3 \mod 4$. \hfill \square

The proofs of Theorems 3.3 and 3.5 did not use square patterns, but they relied on there being just two possible remainders for primes modulo 3 other than 3 and primes modulo 4 other than 4: 1 and another choice. If we try to extend the proofs of those cases to other moduli we quickly run into problems.\footnote{For modulus 6 there is not a problem: the same ideas show there are infinitely many primes $p \equiv 5 \mod 6$. But this is not interesting since for odd $p$ the condition $p \equiv 5 \mod 6$ is the same as the condition $p \equiv 2 \mod 3$, and we already handled this in Theorem 3.3.} For example, if we want to show there are infinitely many primes $p \equiv 4 \mod 5$ then we could observe there are such primes, like 19, and if $p_1, \ldots, p_r$ are all $\equiv 4 \mod 5$ then the product $N = 5p_1 \cdots p_r - 1$ satisfies $N > 1$ and $N \equiv -1 \equiv 4 \not\equiv 1 \mod 5$, so $N$ has a prime factor $p$ that is not $\equiv 1 \mod 5$, but this doesn’t mean $p \equiv 4 \mod 5$. For example, $5 \cdot 19 - 1 = 94 = 2 \cdot 47$ has both prime factors $\equiv 2 \mod 5$.

To extend Euclid’s proof of the infinitude of primes in arithmetic progressions to moduli besides 3 and 4 we will use quadratic expressions to define $N$ in the proof (by comparison, the formula for $N$ in Theorems 3.3 and 3.5 is linear in the product $p_1 \cdots p_r$). This was already seen in Theorems 3.2 and 3.4.

Theorem 3.6. There are infinitely many primes $p \equiv 4 \mod 5$.\footnote{For modulus 6 there is not a problem: the same ideas show there are infinitely many primes $p \equiv 5 \mod 6$. But this is not interesting since for odd $p$ the condition $p \equiv 5 \mod 6$ is the same as the condition $p \equiv 2 \mod 3$, and we already handled this in Theorem 3.3.}
Proof. One such prime is 19. If \( p_1, \ldots, p_r \) are primes \( \equiv 4 \mod 5 \), let
\[
N = (2p_1p_2 \cdots p_r)^2 - 5 > 1.
\]
Then \( N \) is not divisible by 2, 5, or \( p_1, \ldots, p_r \). Let \( p \) be any prime factor of \( N \), so \( 5 \equiv \square \mod p \) (why?). Therefore, since \( p \neq 2 \) or 5, the pattern for \( 5 \equiv \square \mod p \) tells us \( p \equiv 1 \) or 4 \( \mod 5 \): all prime factors of \( N \) are 1 \( \mod 5 \) or 4 \( \mod 5 \). To show \( N \) has a prime factor that is 4 \( \mod 5 \), we argue by contradiction. If every prime factor of \( N \) is 1 \( \mod 5 \), then \( N \equiv 1 \mod 5 \), but in fact \( N \equiv 4 \mod 5 \) since \( p_i^2 \equiv 1 \mod 5 \) for all \( i \). (Here we use \( p_i \equiv 4 \mod 5 \).) Therefore some prime factor \( p \) of \( N \) is not 1 \( \mod 5 \). The only option left is that this prime factor is 4 \( \mod 5 \). This prime is different from \( p_1, \ldots, p_r \), since \( N \equiv -5 \not\equiv 0 \mod p_i \) while \( N \equiv 0 \mod p \), so there are infinitely many primes \( \equiv 4 \mod 5 \). \( \square \)

**Theorem 3.7.** There are infinitely many primes \( p \equiv 3 \mod 8 \).

**Proof.** One such prime is 3. If \( p_1, \ldots, p_r \) are primes \( \equiv 3 \mod 8 \), let
\[
N = (p_1p_2 \cdots p_r)^2 + 2 > 1.
\]
Then \( N \) is not divisible by 2 or by any of \( p_1, \ldots, p_r \). Let \( p \) be any prime factor of \( N \), so \( -2 \equiv \square \mod p \). Therefore, since \( p \neq 2 \), the pattern for \( -2 \equiv \square \mod p \) says \( p \equiv 1 \) or 3 \( \mod 8 \). We want to show \( N \) has a prime factor that is 3 \( \mod 8 \), and will show this by contradiction. If every prime factor of \( N \) is \( \equiv 1 \) \( \mod 8 \), then \( N \equiv 1 \mod 8 \), but in fact \( N \equiv 3 \mod 8 \) since \( p_i^2 \equiv 1 \mod 8 \) for all \( i \). Therefore some prime factor \( p \) of \( N \) is not 1 \( \mod 8 \), so \( p \equiv 3 \mod 8 \). This prime is different from \( p_1, \ldots, p_r \), since \( N \equiv 2 \not\equiv 0 \mod p_i \) while \( N \equiv 0 \mod p \), so there are infinitely many primes \( \equiv 3 \mod 8 \). \( \square \)

**Theorem 3.8.** There are infinitely many primes \( p \equiv 5 \mod 8 \).

**Proof.** One such prime is 5. If \( p_1, \ldots, p_r \) are primes \( \equiv 5 \mod 8 \), let
\[
N = (2p_1p_2 \cdots p_r)^2 + 1 > 1.
\]
Then \( N \) is not divisible by 2 or by any of \( p_1, \ldots, p_r \). Let \( p \) be any prime factor of \( N \), so \( -1 \equiv \square \mod p \). Therefore, since \( p \neq 2 \), we have \( p \equiv 1 \mod 4 \), which is the same as \( p \equiv 1 \) or 5 \( \mod 8 \). If every prime factor of \( N \) is 1 \( \mod 8 \), then \( N \equiv 1 \mod 8 \), but in fact \( N \equiv 5 \mod 8 \) since \( p_i^2 \equiv 1 \mod 8 \) for all \( i \). Therefore some prime factor \( p \) of \( N \) is not 1 \( \mod 8 \), so \( p \equiv 5 \mod 8 \). This prime is different from \( p_1, \ldots, p_r \), since \( N \equiv 1 \not\equiv 0 \mod p_i \) while \( N \equiv 0 \mod p \), so there are infinitely many primes \( \equiv 5 \mod 8 \). \( \square \)

**Theorem 3.9.** There are infinitely many primes \( p \equiv 7 \mod 8 \).

**Proof.** One such prime is 7. If \( p_1, \ldots, p_r \) are primes \( \equiv 7 \mod 8 \), let
\[
N = (p_1p_2 \cdots p_r)^2 - 2 > 1.
\]
Then \( N \) is not divisible by 2 or by any of \( p_1, \ldots, p_r \). Let \( p \) be a prime factor of \( N \), so \( 2 \equiv \square \mod p \). Therefore, since \( p \neq 2 \), the pattern for \( 2 \equiv \square \mod p \) implies \( p \equiv 1 \) or 7 \( \mod 8 \). If every prime factor of \( N \) is 1 \( \mod 8 \), then \( N \equiv 1 \mod 8 \), but in fact \( N \equiv -1 \mod 8 \) since \( p_i^2 \equiv 1 \mod 8 \). Therefore some prime factor \( p \) of \( N \) is not 1 \( \mod 8 \), so \( p \equiv 7 \mod 8 \). This prime is different from \( p_1, \ldots, p_r \), since \( N \equiv -2 \not\equiv 0 \mod p_i \) while \( N \equiv 0 \mod p \), so there are infinitely many primes \( \equiv 7 \mod 8 \). \( \square \)

**Theorem 3.10.** There are infinitely many primes \( p \equiv 5 \mod 12 \).
Proof. One such prime is 5. If \( p_1, \ldots, p_r \) are primes \( \equiv 5 \mod 12 \), let
\[
N = (2p_1p_2 \cdots p_r)^2 + 1 > 1.
\]
Then \( N \) is not divisible by 2 or by any of \( p_1, \ldots, p_r \). Let \( p \) be any prime factor of \( N \), so \(-1 \equiv \square \mod p\). Therefore, since \( p \neq 2 \), we have \( p \equiv 1 \mod 4 \), which is the same as \( p \equiv 1 \) or 5 mod 12. (The choice \( p \equiv 9 \mod 12 \) is satisfied by no prime.) If every prime factor of \( N \) is 1 mod 12, then \( N \equiv 1 \mod 12 \), but in fact \( N \equiv 5 \mod 12 \) since \( p_i^2 \equiv 1 \mod 12 \) for all \( i \). Therefore some prime factor \( p \) of \( N \) is not 1 mod 12, \( p \equiv 5 \mod 12 \). This prime is different from \( p_1, \ldots, p_r \), since \( N \equiv 1 \not\equiv 0 \mod p_i \) while \( N \equiv 0 \mod p \), so there are infinitely many primes \( \equiv 5 \mod 12 \). \( \square \)

Theorem 3.11. There are infinitely many primes \( p \equiv 7 \mod 12 \).

Proof. One such prime is 7. If \( p_1, \ldots, p_r \) are primes \( \equiv 7 \mod 12 \), let
\[
N = (2p_1 \cdots p_r)^2 + 3.
\]
Then \( N \) is not divisible by 2 or by any of \( p_1, \ldots, p_r \). Let \( p \) be any prime factor of \( N \), so \(-3 \equiv \square \mod p\). Therefore, since \( p \) is not 2 or 3, the pattern for \(-3 \equiv \square \mod p\) implies \( p \equiv 1 \mod 3 \). Lifting this mod 3 congruence to modulus 12 tells us \( p \equiv 1, 4, 7 \) or 10 mod 12. No primes are 4 mod 12 or 10 mod 12, so \( p \equiv 1 \) or 7 mod 12. If every prime factor of \( N \) is \( \equiv 1 \mod 12 \), then \( N \equiv 1 \mod 12 \), but in fact \( N \equiv 7 \mod 12 \) since \( p_i^2 \equiv 1 \mod 12 \) for all \( i \) (so \( N \equiv 4 + 3 \mod 12 \)). Therefore some prime factor \( p \) of \( N \) is not 1 mod 12, so \( p \equiv 7 \mod 12 \). This prime is different from \( p_1, \ldots, p_r \), since \( N \equiv 3 \neq 0 \mod p_i \) while \( N \equiv 0 \mod p \), so there are infinitely many primes \( \equiv 7 \mod 12 \). \( \square \)

Theorem 3.12. There are infinitely many primes \( p \equiv 11 \mod 12 \).

Proof. One such prime is 11. If \( p_1, \ldots, p_r \) are primes \( \equiv 11 \mod 12 \), let
\[
N = 3(p_1p_2 \cdots p_r)^2 - 4 > 1.
\]
Then \( N \) is not divisible by 2, 3, or any of \( p_1, \ldots, p_r \). Let \( p \) be a prime factor of \( N \), so \( 3 \equiv \square \mod p \) (why?). Therefore, since \( p \neq 2 \) or 3, the pattern for \( 3 \equiv \square \mod p \) implies \( p \equiv 1 \) or 11 mod 12. If every prime factor of \( N \) is 1 mod 12, then \( N \equiv 1 \mod 12 \), but in fact \( N \equiv -1 \mod 12 \) since \( p_i^2 \equiv 1 \mod 12 \) for all \( i \). Therefore some prime factor \( p \) of \( N \) is not 1 mod 12, so \( p \equiv 11 \mod 12 \). This prime is different from \( p_1, \ldots, p_r \), since \( N \equiv -4 \neq 0 \mod p_i \) while \( N \equiv 0 \mod p \), so there are infinitely many primes \( \equiv 11 \mod 12 \). \( \square \)

In all these proofs, we used a polynomial whose values on integers have special congruence conditions on their prime factors, e.g., to show \( p \equiv 4 \mod 5 \) infinitely often we relied on the fact that any integer of the form \( n^2 - 5 \) with \( n \) even and \( n \neq 0 \mod 5 \) is only divisible by primes \( p \equiv 1, 4 \mod 5 \): if \( p \mid (n^2 - 5) \) then 5 mod \( p \) is a square, so \( p \equiv 1, 4 \mod 5 \) if \( p \neq 2, 5 \). Thus the proof of Theorem 3.6 relies on a feature of the polynomial \( T^2 - 5 \). The table below is a summary of the polynomial and the square condition used for each congruence condition above. Euclid’s proof of the infinitude of the primes is associated to the linear polynomial \( T + 1 \). (Recall the role of \( p_1 \cdots p_r + 1 \) in that proof.) The proofs using square patterns all involve a quadratic polynomial.
We have proved Dirichlet’s theorem (Theorem 3.1) for all cases where $m = 3, 4, 5, 8,$ and 12 except for $1, 2, 3 \mod 5, 1 \mod 8,$ and $1 \mod 12$. These remaining cases for $m = 5, 8,$ and 12 can be handled by elementary techniques in the style we used above, but we have to replace quadratic polynomials with higher degree polynomials. We do not discuss this further here.

## 4. Unsolved Prime Patterns

While an arithmetic progression $a, a+m, a+2m, \ldots$ with $(a, m) = 1$ and $m > 0$ is known to contain infinitely many primes, by Dirichlet’s theorem, there are other sequences that are expected (but not yet known) to contain infinitely many primes. The general principle is that a sequence of integers should contain prime values infinitely often “except when it obviously can’t.” We list a few examples here to illustrate how number theory gives rise to easily stated unsolved problems.

All primes other than 2 are odd and therefore the smallest possible gap between a pair of primes greater than 2 is 2. Primes that differ by 2, such as 3 and 5, 11 and 13, or 1787 and 1789, are called twin primes.

**Conjecture 4.1.** There are infinitely many twin primes.

Do even numbers greater than 2 occur as a prime gap infinitely often?\(^2\) Examples of prime pairs that differ by 4 include 3 and 7, 7 and 11, and 1783 and 1787. Prime pairs that differ by 6 include 5 and 11, 7 and 13, and 1783 and 1789.

**Conjecture 4.2.** For each positive even integer $k$, there are infinitely many pairs of primes that differ by $k$.

Conjecture 4.2 (with Conjecture 4.1 as a special case) was first stated by de Polignac \([6]\) in 1849. By work of Maynard, Tao, Zhang, and others announced during 2013 and 2014, it is known that Conjecture 4.2 is true for infinitely many even $k$, and in particular for some even $k \leq 246 \,[7]\), but it is not yet proved for any specific value of $k$. Before 2013 it had not been known that the gap between pairs of primes could be below any specific 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 any integer $n$ at least one of the numbers $n, n+2, n+4$ is 0 mod 3, and hence such a triple can’t be all prime except when one of them is 3. On the

\(^{2}\text{An odd number can only be a prime gap if one of the primes is 2, so it can occur at most once: 2 and 3 are the only primes that differ by 1, 2 and 5 are the only primes that differ by 3, and no primes differ by 7.}\)
other hand, there is no obvious reason there can’t be infinitely many prime triples of the form \( p, p + 2, \) and \( p + 6, \) and it is believed that there should be infinitely many of these, but this problem lies deeper than the infinitude of twin primes since the first two terms is a pair of twin primes.

More generally, we can ask when a \( k \)-tuple of positive integers \( n + h_1, n + h_2, \ldots, n + h_k, \)
for fixed \( h_1, \ldots, h_k \) in \( \mathbb{Z}, \) should all be prime infinitely often as \( n \) runs over \( \mathbb{Z}^+. \) From what we discussed above, this is expected (but unproved) for \( n, n + 2 \) and for \( n, n + 2, n + 6, \) and is not true for \( n, n + 2, n + 4. \) The only condition that is believed to prevent such \( k \)-tuple sequences from having all prime values infinitely often is when there is a prime \( p \) such that, for all \( n, \) 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 \( n + h_i \equiv 0 \mod p \) is the same as \( -n \equiv h_i \mod p, \) the obstruction to \( n + h_1, n + h_2, \ldots, n + h_k \) all being prime infinitely often due to at least one of them always being divisible by a certain prime \( p \) is that \( \{h_1, h_2, \ldots, h_k \mod p\} \) fills up \( \mathbb{Z}/(p), \) e.g., \( n, n + 2, \) and \( n + 4 \) are not all prime infinitely often due to an obstruction at 3: \( \{1, 2, 4 \mod 3\} = \mathbb{Z}/(3). \) We only need to check for such an obstruction at primes \( p \leq k \) since \( k \) integers can’t fill up \( \mathbb{Z}/(p) \) when \( k > p. \)

**Example 4.3.** 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 last row of the table below 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 \( n = 5. \)

\[
\begin{array}{cccccccc}
p & 0 \mod p & 2 \mod p & 6 \mod p & 8 \mod p & 12 \mod p & 14 \mod p \\
2 & 0 & 0 & 0 & 0 & 0 & 0 \\
3 & 0 & 2 & 0 & 2 & 0 & 2 \\
5 & 0 & 2 & 1 & 3 & 2 & 4 \\
\end{array}
\]

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

\[
\begin{array}{cccccccc}
p & 0 \mod p & 2 \mod p & 6 \mod p & 8 \mod p & 12 \mod p & 18 \mod p \\
2 & 0 & 0 & 0 & 0 & 0 & 0 \\
3 & 0 & 2 & 0 & 2 & 0 & 0 \\
5 & 0 & 2 & 1 & 3 & 2 & 3 \\
\end{array}
\]

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.

**Conjecture 4.4.** For \( h_1, h_2, \ldots, h_k \) in \( \mathbb{Z}, \) there are infinitely many prime \( k \)-tuples \( n + h_1, n + h_2, \ldots, n + h_k \) if there is no prime \( p \leq k \) such that \( \{h_1, \ldots, h_k \mod p\} = \mathbb{Z}/(p). \)

This conjecture was first made by Dickson [2] in 1904. Dickson actually considered a more general setup, for prime values of \( k \) linear expressions \( a_1 n + b_1, \ldots, a_k n + b_k, \) which for \( k = 1 \) becomes Dirichlet’s theorem (the only explicit proved case of Conjecture 4.4). The work of Maynard and Tao [5] implies that, for each \( k, \) Conjecture 4.4 is true for infinitely many \( \{h_1, \ldots, h_k\}, \) but it is not known for any explicit \( k \)-tuple when \( k \geq 2. \)

\[^3\text{About 20 years later Hardy and Littlewood formulated a quantitative version of Conjecture 4.4, predicting about how many } n \leq x \text{ make the } k \text{-tuple all prime, as } x \text{ grows. Therefore this conjecture is often attributed to Hardy and Littlewood.} \]
What about prime values of higher-degree polynomials?

**Conjecture 4.5.** 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 10,000 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. It was included much later by Landau [4, p. 106] in a 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.

Replacing linear polynomials with higher-degree polynomials, Schinzel’s “Hypothesis H” [8] (1958) predicts when a \( k \)-tuple of polynomial values \( (f_1(n), f_2(n), \ldots, f_k(n)) \) should be prime infinitely often. No instance of it is known other than a single linear polynomial (Dirichlet’s theorem).

A number of the form \( a^n - 1 \) can be prime only if \( a = 2 \) and \( n = p \) is prime, although not all numbers of the form \( 2^p - 1 \) have to be prime, e.g., \( 2^{11} - 1 = 23 \cdot 89 \) and \( 2^{23} - 1 = 47 \cdot 178481 \). Any prime of the form \( 2^p - 1 \) is called a *Mersenne prime* after Marin Mersenne. The first ten Mersenne primes \( 2^p - 1 \) occur for \( p = 2, 3, 5, 7, 13, 17, 19, 31, 61, \) and 89.

**Conjecture 4.6.** There are infinitely many Mersenne primes.

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 occurring for \( p = 82,589,933 \) It 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.

Aside from Mersenne primes \( 2^n - 1 \), we can consider primes of the form \( 2^n - 3 \), \( 2^n - 5 \), and more generally \( 2^n - k \) for odd positive integers \( k \). For small odd \( k \), the first six \( n \) making \( 2^n - k \) prime are in the table below along with a link to a table at the Online Encyclopedia of Integer Sequences (OEIS) where the list of exponents continues.

<table>
<thead>
<tr>
<th>( k )</th>
<th>( n \geq 1 ) making ( 2^n - k ) prime</th>
<th>OEIS link</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2, 3, 5, 7, 13, 17, \ldots</td>
<td><a href="https://oeis.org/A000043">https://oeis.org/A000043</a></td>
</tr>
<tr>
<td>3</td>
<td>3, 4, 5, 6, 9, 10, \ldots</td>
<td><a href="https://oeis.org/A050414">https://oeis.org/A050414</a></td>
</tr>
<tr>
<td>5</td>
<td>3, 4, 6, 8, 10, 12, \ldots</td>
<td><a href="https://oeis.org/A059608">https://oeis.org/A059608</a></td>
</tr>
<tr>
<td>7</td>
<td>39, 715, 1983, 2319, 2499, 3775, \ldots</td>
<td><a href="https://oeis.org/A059609">https://oeis.org/A059609</a></td>
</tr>
<tr>
<td>9</td>
<td>4, 5, 9, 11, 17, 21, \ldots</td>
<td><a href="https://oeis.org/A059610">https://oeis.org/A059610</a></td>
</tr>
</tbody>
</table>

Initial prime values of \( 2^n - 7 \) occur much farther out than the other sequences. Its primality at \( n = 39 \) was verified by T. Kulikowski in 1960. He showed \( 2^{39} - 7 \) is prime by showing (with a computer) that it has the form \( a^2 + b^2 \) with \( (a, b) = 1 \) in just one way.

Switching from \( 2^n - k \) to \( 2^n + k \) for odd positive integers \( k \), below is a table of the first six \( n \geq 1 \) making \( 2^n + k \) prime for small \( k \).

<table>
<thead>
<tr>
<th>( k )</th>
<th>( n \geq 1 ) making ( 2^n + k ) prime</th>
<th>OEIS link</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1, 2, 4, 8, 16, \ldots</td>
<td><a href="https://oeis.org/A057732">https://oeis.org/A057732</a></td>
</tr>
<tr>
<td>3</td>
<td>1, 2, 3, 4, 6, 7, \ldots</td>
<td><a href="https://oeis.org/A057732">https://oeis.org/A057732</a></td>
</tr>
<tr>
<td>5</td>
<td>1, 3, 5, 11, 47, 53, \ldots</td>
<td><a href="https://oeis.org/A059242">https://oeis.org/A059242</a></td>
</tr>
<tr>
<td>7</td>
<td>2, 4, 6, 8, 10, 16, \ldots</td>
<td><a href="https://oeis.org/A057195">https://oeis.org/A057195</a></td>
</tr>
<tr>
<td>9</td>
<td>1, 2, 3, 5, 6, 7, \ldots</td>
<td><a href="https://oeis.org/A057196">https://oeis.org/A057196</a></td>
</tr>
</tbody>
</table>
The first row there looks different from the rest: only 5 examples are known. Primes of the form $2^n + 1$ are called Fermat primes. While $2^n - 1$ can only be prime when $n$ is prime, $2^n + 1$ can only be prime when $n$ is a power of 2. Fermat knew $2^n + 1$ is prime when $n$ is 1, 2, 4, 8, and 16, and conjectured it is prime when $n$ is any power of 2, but he was mistaken: Euler, in 1732, proved $2^{32} + 1$ has factor 641. It is now believed that there are no Fermat primes beyond the first five. The other lists in the tables above are expected, but not proved, to be infinite.

Switching from $2^n \pm k$ to $k \cdot 2^n \pm 1$, there are odd $k$ where all the numbers of that form are provably composite! Hans Riesel showed in 1956 that $k \cdot 2^n - 1$ is composite for all $n \geq 1$ if $k = 509203$ and the same result is true for infinitely many larger odd $k$. It is not yet known if 509203 is the smallest such $k$; for example, when $k = 2293$ no prime value of $k \cdot 2^n - 1$ has been found but it is not proved that those numbers are never prime. In 1960, Waclaw Sierpinski proved with the Chinese remainder theorem that there are infinitely many odd $k$ such that $k \cdot 2^n + 1$ is composite for all $n \geq 1$, and the smallest $k$ from his method is 15511380746462593381. John Selfridge showed in 1962 that $k \cdot 2^n + 1$ is composite for all $n \geq 1$ when $k = 78557$ and it is conjectured that 78557 is the smallest such $k$.

Appendix A. The Logic Behind Dirichlet’s Theorem

Dirichlet’s theorem says there are infinitely many primes satisfying $p \equiv a \mod m$ when $(a, m) = 1$. It’s not any easier to show there is even one prime $p \equiv a \mod m$. In fact, that turns out to be just as hard as Dirichlet’s theorem!

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

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

This is very surprising. The theorem seems to be saying, for instance, that by knowing there is one prime $p \equiv 4 \mod 7$, like $p = 11$, it follows that there are infinitely many primes $p \equiv 4 \mod 7$. 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 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 $p_1 \equiv a \mod m$. We want to show there are infinitely many primes $p \equiv a \mod m$. 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 “$p \equiv a \mod m$” 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 $p \equiv 8 \mod 5$, look at it as $p \equiv 3 \mod 5$; that’s the same thing.)

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

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

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 $p \equiv a \mod m$. 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 $p \equiv 8 \mod 5$ 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 $p \equiv a \mod m$ 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 $p \equiv a \mod m$ by computation, the only known way to prove there is a prime $p \equiv a \mod m$ whenever $(a, m) = 1$ is to prove there are infinitely many such primes.

References


