Infinitely many composites

NICK LORD, DES MacHALE

Introduction

In number theory, we frequently ask if there are infinitely many prime numbers of a certain type. For example, if n is a natural number:

(i) Are there infinitely many (Mersenne) primes of the form $2^n - 1$?

(ii) Are there infinitely many primes of the form $n^2 + 1$?

These problems are often very difficult and many remain unsolved to this day, despite the efforts of many great mathematicians. However, we can sometimes comfort ourselves by asking if there are infinitely many composite numbers of a certain type. These questions are often (but not always) easier to answer. For example, echoing (i) above, we can ask if there are infinitely many composites of the form $2^p - 1$ with p a prime number but (to the best of our knowledge) this remains an unsolved problem. Of course, it must be the case that there are either infinitely many primes or infinitely many composites of the form $2^p - 1$ and it seems strange that we currently cannot decide on either of them.

In this Article, we concentrate on the question, “Are there infinitely many composite numbers of a certain type?”. In most cases we give proofs that there are, while in other cases we quote the results of calculations or make conjectures. Most of the specific numerical examples are essentially templates that may readily be generalised. Our methods will be mainly elementary and similar to those employed in our previous articles, [1, 2, 3], with one exception. In several places, we have made judicious use of Dirichlet's wonderful and powerful theorem that, if a and b are coprime integers, then the arithmetic sequence $\{a + nb : n = 0, 1, 2, \dots \}$ contains infinitely many primes. (For a self-contained account of the proof of Dirichlet's theorem aimed at the general reader, we recommend Martin Griffiths' book, [4].)

Polynomial sequences

The behaviour of some polynomial sequences may be immediately apparent.

- The sequence $\{n^2 + n + 2\}$ consists of composite even numbers for $n \geqslant 1$, since $n^2 + n + 2 = n(n + 1) + 2$.
- The polynomial $n^4 + 4 = (n^2 + 2)^2 - (2n)^2 = (n^2 - 2n + 2)(n^2 + 2n + 2)$ factorises to show that the sequence $\{n^4 + 4\}$ consists of composite numbers for $n \geqslant 2$.
- The sequence $\{n^2 + n + 1\}$ contains the subsequence $\{k^4 + k^2 + 1\}$ of composite numbers for $k \geqslant 2$ since $k^4 + k^2 + 1 = (k^2 + 1)^2 - k^2 = (k^2 - k + 1)(k^2 + k + 1)$.
- Consider the sequence $\{n^2 + 1\}$, mod 10.
For $n \equiv 1, 3, 5, 7, 9 \pmod{10}$, $n^2 + 1 \equiv 0 \pmod 2$ and so is composite for $n > 1$.

https://doi.org/10.1017/mag.2024.4 Published online by Cambridge University Press

> For $n \equiv 2, 8 \pmod{10}$, $n^2 + 1 \equiv 0 \pmod 5$ and so is composite for $n > 2$.
>
> Question (ii) in the introduction may thus be refined to ask: Are there infinitely many prime numbers of the form $n^2 + 1$ for $n \equiv 0, 4, 6 \pmod{10}$?

We now give two useful general results on polynomial sequences.

Theorem 1

Let $f(x)$ be a non-constant polynomial with integer coefficients. Then $f(n)$ is composite for infinitely many positive and infinitely many negative values of n.

Proof: If $f(n)$ is composite for all integer values of n, we are done. Otherwise, $f(m) = p$, prime, for some integer m. Then, if $f(x) = a_0 + a_1x + \dots + a_rx^r$, $f(m + kp) - f(m) = \sum_{i=1}^{r} a_i\left[(m + kp)^i - m^i\right]$ with $(m + kp)^i - m^i$ divisible by $m + kp - m = kp$. Thus $f(m + kp) - f(m)$ is divisible by p and $f(m + kp)$ is divisible by p for all integers k which establishes the result.

Theorem 2

Let $a, b > 0$ be two coprime integers.

(a) There are infinitely many composite numbers of the form $a + bn$.

(b) There are infinitely many composite numbers of the form $a + bp$ with p prime.

Proof:

(a) There are several ways of seeing this: one is to let $n = a\left(2k + bk^2\right)$. Then $a + bn = a\left(1 + 2kb + b^2k^2\right) = a(1 + kb)^2$, which is composite for all $k \geqslant 2$.

(b) By Dirichlet's theorem in the introduction, there are infinitely many prime numbers of the form $a + bn$, $n \geqslant 0$: pick one, say $a + bq = p$. Then p and q are coprime because $p > q$ and p is prime. By Dirichlet again, there are infinitely many primes of the form $q + np$ for which $a + b(q + np) = p(1 + nb)$ is composite for all $n \geqslant 1$.

It is not known whether there are infinitely many *Sophie Germain primes* p for which $2p + 1$ is also prime. Similarly, it is not known whether there are infinitely many primes p for which $2p - 1$ is also prime. But Theorem 2(b) guarantees that there are infinitely many primes for which $2p - 1$ is composite and (separately) infinitely many primes for which $2p + 1$ is composite. Indeed, we can tweak Theorem 2(b) to show that there are infinitely many primes p for which $2p - 1$ and $2p + 1$ are simultaneously composite. For, by Dirichlet's theorem, since 2 and 15 are coprime, there are infinitely many primes of the form $p = 15k + 2$ for which $2p - 1 = 30k + 3$ is a multiple of 3 and $2p + 1 = 30k + 5$ is a multiple of 5.

(A similar proof may be constructed from any pair of twin primes in place of 3 and 5.)

https://doi.org/10.1017/mag.2024.4 Published online by Cambridge University Press

It is also possible to prove results analogous to that in Theorem 2(b) for non-linear polynomials. For example, although it is not known whether, for fixed $a \geqslant 1$, there are infinitely many primes of the form $n^2 + 2a$, we can show that there are infinitely many such composite numbers in which n is prime. For let $q > 1$ be any factor of $2a + 1$. Then, by Dirichlet's theorem, there are infinitely many primes p of the form $p = 1 + kq$ for which $p^2 + 2a = kq(kq + 2) + (2a + 1)$ is divisible by q. A similar argument, using $q > 1$ any factor of $a + b$ for coprime positive integers a, b, shows that there are infinitely many composite numbers of the form $a + bp^2$ with p prime.

The following puzzle seems a fitting note on which to end this section.

For prime numbers p, show that $p^2 - 1 + 3n$ *is composite for all n, except when* $p = 3$.

We consider cases which cover all prime numbers.

For $p = 6k \pm 1$, $p^2 - 1 + 3n = 12k(3k \pm 1) + 3n$, which is divisible by 3.

For $p = 2$, $p^2 - 1 + 3n = 3(n + 1)$ is also divisible by 3.

But if $p = 3$, then $p^2 - 1 + 3n = 8 + 3n$ takes prime values infinitely often, by Dirichlet's theorem.

Sequences of factorials

In this section, we collate some illustrative examples.

- $n! + 1$ is composite for infinitely many values of n.
  For, by Wilson's theorem, $(p - 1)! + 1 \equiv 0 \pmod p$ for all primes p, and $(p - 1)! + 1 > p$ for all $p \geqslant 5$.
- $n! - 1$ is composite for infinitely many values of n.
  For, by Wilson's theorem, $(p-1)! + 1 = p(p-2)! - (p-2)! + 1$ so that $1 - (p - 2)! \equiv (p - 1)! + 1 \equiv 0 \pmod p$. So p divides $(p - 2)! - 1$ and $(p - 2)! - 1 > p$ for $p \geqslant 7$.

But are there infinitely many values of n for which $n! - 1$ and $n! + 1$ are both composite?

And is $n = 3$ the only value of n for which $n! - 1$ and $n! + 1$ are both prime?

For some closely related sequences, the behaviour is easier to decide.

- There are infinitely many values of n for which $n! - (n + 1)$ and $n! + (n + 1)$ are both composite.
  We can see this algebraically. For example, $\left(k^2 - 2\right)! \pm \left(k^2 - 1\right)$ is divisible by $k - 1$ and $k + 1$. And, more generally, $(rs - 1)! \pm rs$ is divisible by r and by s.
- $1! + 2! + 3! + \dots + n!$ is composite infinitely often since it is divisible by 3 for all $n \geqslant 2$.

https://doi.org/10.1017/mag.2024.4 Published online by Cambridge University Press

- But $1! + 3! + 5! + \ldots + (2n - 1)!$ is harder to pin down.
  It turns out that $1! + 3! + 5! + \ldots + 105! \equiv 0 \pmod{107}$ so, incredibly, $1! + 3! + 5! + \ldots + (2n - 1)!$ is divisible by 107 for all $n \geqslant 53$.

Sequences of powers

We begin by reprising and extending two familiar results.

- If $2^n - 1$ is prime, then n is prime.
  For if $n = rs$ is composite, then the algebraic fact that $x - 1$ divides $x^s - 1$ means that $2^r - 1$ divides $2^{rs} - 1$.
- If $2^n + 1$ is prime, then n is power of 2.
  For if $n = rs$ has an odd factor $s > 1$, then the algebraic fact that $x + 1$ divides $x^s + 1$ means that $2^r + 1$ divides $2^{rs} + 1$.

Of course, the converses of these results are not true, and it is not known whether there are infinitely many primes/composites of these two respective types. But there are infinitely many values of n for which $2^n - 1$ and $2^n + 1$ are both composite: any n that is neither prime nor a power of 2 suffices. (An explicit example would be $n = 3k$ for $k > 2$, where the algebraic fact that $x \pm 1$ divides $x^3 \pm 1$ means that $2^{3k} \pm 1$ are both composite.)

If we replace 2 with $a > 2$, $a^n - 1$ is always composite for $n > 1$ since it is divisible by $a - 1$, but the proof above shows that if $a^n + 1$ is prime, then n is a power of 2. It is thus tempting to make a conjecture mimicking that for Fermat primes – that $a^{2^n} + 1$ is only prime for finitely many values of n. For specific values of a, the evidence may point this way (for example, $10^{2^n} + 1$ is prime for $n = 0, 1$ but composite for $2 \leqslant n \leqslant 23$).

But in general such a conjecture is false: $8^{2^n} + 1$ is composite for all $n \geqslant 0$ because the algebraic fact that $x + 1$ divides $x^3 + 1$ means that $8^{2^n} + 1 = 2^{3.2^n} + 1$ is divisible by $2^{2^n} + 1$.

Related sequences are also interesting to investigate.

- $a_n = 11 \times 14^n + 1$ is composite for all $n \geqslant 0$.
  For $a_n \equiv 1 \times (-1)^n + 1 \pmod 5$ and $a_n \equiv (-1) \times (-1)^n + 1 \pmod 3$ so that $a_n \equiv 0 \pmod 5$ if n is odd, while $a_n \equiv 0 \pmod 3$ if n is even.
- $3^n - 2$ and $3^n + 2$ are each composite for infinitely many values of n.
  The final decimal digits of 3^n, $n \geqslant 0$, consist of the repeating block of four digits 1, 3, 9, 7. If the final digit is 7, then $3^n - 2$ is divisible by 5; if it is 3, then $3^n + 2$ is divisible by 5.
- We are indebted to the referee for suggesting the following general result of this type. Let a, b, c be positive integers with $a > 1$ and a, c coprime. Then $a^n b + c$ is composite for infinitely many values of n.
  To see this, let $r = ab + c$. Then a and r are coprime so, by the Euler-Fermat theorem, $a^k \equiv 1 \pmod r$, where $k = \phi(r)$. Then, for all

https://doi.org/10.1017/mag.2024.4 Published online by Cambridge University Press

$n \geqslant 1$, $a^{nk+1} \equiv a \pmod r$ and $a^{nk+1}b + c \equiv ab + c = r \pmod r$, so is always divisible by r. This argument also works for $c < 0$ unless $ab + c = \pm 1$, in which case we may take $r = a^2 b + c$ and consider $a^{nk+2}b + c$.

- $2^{2^n} + 3$ is composite for infinitely many values of n.
  For $2^{2k} \equiv 1 \pmod 3$ so that $2^{2k+1} = 3r + 2$. Then
  $2^{2^{2k+1}} + 3 = 2^{3r+2} + 3 = 4 \times 8^r + 3 \equiv 0 \pmod 7$.

Finally, closer inspection of sequences reveals more subtle aspects of their behaviour.

- For prime p, the first three cases of composite values of $2^p - 1$ are:

$$2^{11} - 1 = 23 \times 89$$

$$2^{23} - 1 = 47 \times 178481$$

$$2^{29} - 1 = 233 \times 2304167.$$

  If the prime q divides $2^p - 1$, then $2^p \equiv 1 \pmod q$ so 2 has order $p \pmod q$.

  It follows that p divides $q - 1$ so that q has the form $q = kp + 1$, as may be checked for the factors above.

  A result originally proved by Euler is that $q = 2p + 1$ is always one such factor if p is a Sophie Germain prime of the form $4k + 3$ (for which $8k + 7$ is also prime). In this situation, 2 is known to be a quadratic residue mod $8k + 7$, say $r^2 \equiv 2 \pmod{8k + 7}$. Then, by Fermat's little theorem, $2^{4k+3} \equiv r^{8k+6} \equiv 1 \pmod{8k + 7}$, so that $8k + 7$ divides $2^{4k+3} - 1$. The first few such Sophie Germain primes are 3, 11, 23, 83, 131; if there are infinitely many such, then there are infinitely many composite Mersenne numbers.

- For odd primes p, $2^p + 1$ is divisible by 3, but $\frac{1}{3}\left(2^p + 1\right)$ is prime for $p = 3, 5, 7, 11, 13, 17, 19, 23, 31$, but not for the 'spoilsport' prime 29 since $\frac{1}{3}\left(2^{29} + 1\right) = 59 \times 3033169$. Again, there is an interesting connection with Sophie Germain primes, this time of the form $4k + 1$ (for which $8k + 3$ is also prime). Fermat's little theorem means that
  $\left(2^{4k+1} - 1\right)\left(2^{4k+1} + 1\right) = 2^{8k+2} - 1 \equiv 0 \pmod{8k + 3}$.
  So $8k + 3$ divides either $2^{4k+1} - 1$ or $2^{4k+1} + 1$. But if $2^{4k+1} \equiv 1 \pmod{8k + 3}$, then $\left(2^{2k+1}\right)^2 \equiv 2 \pmod{8k + 3}$, so 2 would be a quadratic residue mod $8k + 3$, which is known not to be the case. Thus, for Sophie Germain primes of the form $4k + 1$ (such as 29, 41, 53, ...), $8k + 3$ is always a spoilsport factor of $\frac{1}{3}\left(2^{4k+1} + 1\right)$.

https://doi.org/10.1017/mag.2024.4 Published online by Cambridge University Press

Open questions

The following questions struck us as worthy of further investigation.

- Let p_n denote the nth prime.
  Are there infinitely many composites of the forms $p_1 p_2 \dots p_n + 1$, $p_1 p_2 \dots p_n - 1, p_1 p_2 \dots p_n + p_{n+1}, p_1 p_2 \dots p_n - p_{n+1}$?
  Are they both prime only when $p = 2, 3, 5$?
  Are there infinitely many composite pairs of the forms $p_1 p_2 \dots p_n \pm 1, p_1 p_2 \dots p_n \pm p_{n+1}$?

- Let $n^* = \text{LCM}\{1, 2, \dots, n\}$.
  Are there infinitely many composites of the forms $n^* - 1, n^* + 1$?
  Are there infinitely many composite pairs of the forms $n^* \pm 1$?
  Here, $n^* \pm 2, n^* \pm 3, \dots, n^* \pm n$ are all composite, so a natural question is:
  Are there infinitely many composites of the forms $n^* - (n + 1)$, $n^* + (n + 1)$?

- Polynomials in two variables are also of interest: m and n are natural numbers in the following examples.

  There are infinitely many primes of the form $m^2 + n^2$: this follows from Fermat's theorem that every prime of the form $4k + 1$ is the sum of two squares. But there are also clearly infinitely many composites of the form $m^2 + n^2$ because $m^2 + n^2$ is even when m and n have the same parity.

  The polynomial

  $$m^4 + 4n^4 = \left(m^2 + 2n^2\right)^2 - (2mn)^2 = \left(m^2 - 2mn + 2n^2\right)\left(m^2 + 2mn + 2n^2\right)$$

  factorises to show that $m^4 + 4n^4$ is composite except when

  $$1 = m^2 - 2mn + 2n^2 = (m - n)^2 + n^2,$$

  forcing $m = n = 1$.

  Similarly, the polynomial

  $$m^4 + m^2n^2 + n^4 = \left(m^2 + n^2\right)^2 - (mn)^2 = \left(m^2 - mn + n^2\right)\left(m^2 + mn + n^2\right)$$

  factorises to show that $m^4 + m^2n^2 + n^4$ is composite except when $m = n = 1$.

But it is all too easy to over-reach oneself. For example, a natural question is whether, for each n, there is a run of precisely n composite numbers. This is equivalent to asking which differences can occur between prime numbers and, although *Polignac's conjecture* of 1849 asserts that every even number occurs as a difference between primes, it remains unresolved.

https://doi.org/10.1017/mag.2024.4 Published online by Cambridge University Press

Acknowledgements

We are very grateful to Dr Robert Heffernan of Munster Technological University for extensive computing help with the calculations in this paper. We also acknowledge the constant inspiration provided by Neil Sloane's encyclopaedia of integer sequences, [5], a source of information about many of the sequences we have investigated. Finally, we warmly thank the referee for providing the general result on sequences of powers and suggesting that we include Euler's result on Sophie Germain primes.

References

1. N. Lord, Extending runs of composite numbers, *Math. Gaz.* **102** (July 2018) pp. 351-352.
2. D. MacHale, Some elementary results in number theory, *Math. Gaz.* **105** (July 2021) pp. 282-285.
3. N. Lord, On 105.16, *Math. Gaz.* **105** (November 2021) p. 550.
4. M. Griffiths, *A prime puzzle*, United Kingdom Mathematics Trust (2012).
5. The on-line encyclopaedia of integer sequences, https://oeis.org/

10.1017/mag.2024.4 © The Authors, 2024
Published by Cambridge University Press
on behalf of The Mathematical Association

NICK LORD
Tonbridge School,
Kent TN9 1JP
e-mail: *njl@tonbridge-school.org*
DES MacHALE
School of Mathematics, Applied Mathematics and Statistics
University College Cork, Cork, Ireland
e-mail: *d.machale@ucc.ie*

Continued from page 19.

3. The momentum of his motion carried him past her, but an invisible force made up of surprise and curiosity and desire spun him round as soon as he had passed.

4. Besides, it was not fear, but terror, that convulsed him. But the slope grew more gradual, and its base was grass-covered. Here the cub lost momentum.

5. Contemptible details these, to make part of a history; yet the turn of most lives is hardly to be accounted for without them. They are continually entering with cumulative force into a mood until it gets the mass and momentum of a theory or a motive.

6. Then we began to gather momentum, and presently were fairly under way and booming along. It was all as natural and familiar - and and so were the shoreward sights – as if there had been no break in my river life.