Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 74 (2019)
Heft: 1

Artikel: Composite values of irreducible polynomials
Autor: Lemmermeyer, Franz
DOI: https://doi.org/10.5169/seals-869231

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 12.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Elem. Math. 74 (2019) 36 – 37
0013-6018/19/010036-2
DOI 10.4171/EM/378

© Swiss Mathematical Society, 2019

Elemente der Mathematik

Short note Composite values of irreducible polynomials

Franz Lemmermeyer

In his letter to Euler from September 1743 in [3, Letter 73], Goldbach remarked that it

> *is very easy to prove that no algebraic formula such as $a+bx+cx^2+dx^3+\cdots$, where x is the index of the terms, can yield none but prime numbers, whatever integers the coefficients a, b, c, ... may be; but all the same there are formulae which comprise a greater number of primes than many others; the series $x^2+19x-19$ is of this kind, as in its 47 initial terms it comprises only 4 non-prime numbers.*

In this note we will give a very short proof of Goldbach's claim based on a simple identity, which shows not only the existence of infinitely many composite values of a given polynomial, but presents identities from which the claim follows directly. As an example, applying our result to Goldbach's polynomial $f(x) = x^2 + 19x - 19$ provides us with the identity

$$f(x^2 + 20x - 19) = f(x) \cdot g(x) \quad \text{with} \quad g(x) = x^2 + 21x + 1 = f(x+1),$$

which implies that f attains infinitely many composite values. In particular, $f(25) = f(f(2)+2) = f(2) \cdot g(2) = 23 \cdot 47$.

Observe that Goldbach's claim is trivial if f is reducible or if its content (the greatest common divisor of its coefficients) is not a unit. Our main result is the following

Theorem 1. *Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial with integral and coprime coefficients. Then for an arbitrarily chosen polynomial $q(x) \in \mathbb{Z}[x]$ there exists a polynomial $g \in \mathbb{Z}[x]$ such that*

$$f(q(x)f(x) + x) = f(x)g(x). \tag{1}$$

We have to show that for every choice of $q(x) \in \mathbb{Z}[x]$, the polynomial

$$h(x) = f(q(x)f(x) + x)$$

is divisible by $f(x)$. Since f is irreducible, a polynomial h is divisible by f in the ring $\mathbb{Q}[x]$ if and only if $h(\alpha) = 0$ for all the complex roots α of f. But if $f(\alpha) = 0$, then

$$h(\alpha) = f(q(\alpha)f(\alpha) + \alpha) = f(\alpha) = 0,$$

and we are done. Gauss's Lemma for polynomials (see [4] and [2] for the history of this result) now tells us that if $h = fg$ for polynomials $f, h \in \mathbb{Z}[x]$ for a primitive polynomial f, then the coefficients of g must be integral. This completes the proof.

This implies in particular that polynomials f with degree ≥ 1 represent infinitely many composite numbers of the form $f(f(x)+x)$. In fact, assume that $f(x) = a_n x^n + \cdots + a_0$ with $a_n \geq 1$. Then there is a constant $C > 0$ such that $f(x) > 1$ and $f'(x) > 0$ for all $x > C$. But then $f(x) + x > x$, hence $f(f(x) + x) > f(x)$ and thus also $g(x) > 1$.

A second proof. Theorem 1 may also be proved by setting $h = q(x)f(x)$ in the Taylor identity

$$f(x+h) = f(x) + f'(x) \cdot h + \frac{f''(x)}{2!}h^2 + \cdots + \frac{f^{(n+1)}(x)}{(n+1)!}h^{n+1}.$$

This implies

$$f(x+f(x)) = f(x)\left[1+f'(x)q(x)+\frac{f''(x)}{2!}f(x)q(x)^2+\cdots+\frac{f^{(n+1)}(x)}{(n+1)!}f(x)^n q(x)^{n+1}\right].$$

Observe that the polynomials $\frac{1}{k!}f^{(k)}(x)$ have integral coefficients since the product of k consecutive integers is divisible by $k!$.

Applications to Goldbach's polynomial. Out of the four composite values of $f(n)$ for $0 \leq n \leq 47$, where $f(x) = x^2 + 19x - 19$ is Goldbach's polynomial, the numbers $f(19)$ and $f(38)$ (and more generally $f(19k)$ for integers $k \geq 1$) are composite for trivial reasons: they are clearly divisible by 19. The other two composite values are $f(25) = f(2 + f(2))$ and $f(36) = f(-f(-1) - 1)$. The next few composite values also follow from our theorem.

André Gérardin. I was led to the problem addressed here by a remark by André Gérardin (1879–1953) in [1], in which he claimed that the numbers of the form $2a^2-1$ are composite for $a = 9, 89, 881$ etc. I quickly found that these numbers are solutions of the diophantine equation $3a^2 - 2b^2 = 1$, and that Gérardin's claim follows from the observation that

$$9(2x^2 - 1) = 3(4y^2 - 1) = 3(2y - 1)(2y + 1).$$

This is reminiscent of the well-known fact that there are infinitely many composite integers of the form $f(x) = 4x^2 + 1$ since

$$f(a^2) = 4a^4 + 1 = (2a^2 + 1)^2 - 4a^2 = (2a^2 + 2a + 1)(2a^2 - 2a + 1).$$

This begs the question whether there is a result that encompasses all these examples.

References

[1] A. Gerardin, *Méthode inédite de découverte des facteurs d'un nombre composé de grandeur quelconque. Exemples simples*, L'Enseign. math. **21** (1920), 212–213

[2] F. Lemmermeyer, *Zur Zahlentheorie der Griechen. II: Gaußsche Lemmas und Rieszsche Ringe*, Math. Semesterber. **56** (2009), 39–51

[3] F. Lemmermeyer, M. Mattmüller (editors), *Leonhardi Euler Opera Omnia (IV) 4. Correspondence of Leonhard Euler with Christian Goldbach*, Birkhäuser Basel 2015

[4] A. Magidin, D. McKinnon, *Gauss's lemma for number fields*, Am. Math. Mon. **112** (2005), 385–416

Franz Lemmermeyer, Mörikeweg 1, D-73489 Jagstzell, Deutschland
e-mail: `hb3@ix.urz.uni-heidelberg.de`