COMPOSITE VALUES OF IRREDUCIBLE POLYNOMIALS

FRANZ LEMMERMEYER

In his letter to Euler from September 1743 in [2, Letter 73], Goldbach remarked that it

> *is very easy to prove that no algebraic formula such as* $a+bx+cx^2+dx^3+\ldots$, *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*

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

Proof. Since f is irreducible, a polynomial $h\in\mathbb{Z}[x]$ 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

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

and we are done. By Gauss's Lemma for polynomials (see [3] and [1] for the history of this result), the coefficients of h must be integral. □

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 $f(x) = a_nx^n+\ldots+a_0$ with $a_n\ge 1$. 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 $g(x)>1$.

Out of the four composite values of $f(n)$ for $0\le n\le 47$, where $f(x)=x^2+19x-19$ is Goldbach's polynomial, the numbers $f(19)$ and $f(38)$ 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 flow from our theorem: $f(48) = f(2f(2)+2)$, $f(50) = f(f(3)+3)$, and $f(51) = f(-f(-2)-2)$. The smallest composite value I could not derive from (1) is $f(56) = 37 \cdot 113$.

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

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

This implies

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

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

References

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

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

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