

Alfred's Ansatz: Solution

Rewrite $2^{62} + 1$ as $4x^4 + 1$ with $x = 2^{15}$. The polynomial $4x^4 + 1$ has no real root, since x^4 can't be negative, so it cannot have a linear factor, and thus instead must have only quadratic factors (if it factors at all). Indeed, it must be a product of two quadratics. Their leading terms are either both $2x^2$ or else one is x^2 and the other is $4x^2$. Let's look at the first case and if that doesn't pan out explore the second. Write out the factorization

$$4x^4 + 1 = (2x^2 + ax + b)(2x^2 + cx + d).$$

When expanded out and like terms collected, the right-hand side becomes

$$4x^4 + 2(a + c)x^3 + (2b + 2d + ac)x^2 + (ad + bc)x + bd.$$

The coefficient of x^3 must be 0, so $c = -a$. The constant coefficient must be 1, so b and d are either both 1 or both -1 (in particular, $b = d$). We can now substitute $-a$ for c and b for d so there are only two unknowns. The coefficient of x becomes $ab - ba$ which is automatically 0. The coefficient of x^2 is now $4b - a^2$, which must be 0, so $a^2 = 4b$. This forces b to be nonnegative, so $b = 1$ and $a = \pm 2$. Putting this all together we get the factorizations

$$4x^4 + 1 = (2x^2 + 2x + 1)(2x^2 - 2x + 1),$$

$$2^{62} + 1 = (2^{31} + 2^{16} + 1)(2^{31} - 2^{16} + 1).$$

Each of the two factors above would work.

In general, the polynomial $x^n - 1$ (and by extension, $x^n + 1$) can be factored into the irreducible *cyclotomic polynomials* $\Phi_n(x)$. These can be “factored” further in a different sort of way as $\Phi(x) = U(x)^2 \pm \circ V(x)^2$ for polynomials $U(x), V(x)$ and monomial \circ depending on n (due to Lucas, Gauss, Schinzel).

This allows us to factor $\Phi_n(x)$ as an integer for particular values of x , which Aurifeuille (pseudonym Alfred de Caston) did in the case of

$$\begin{aligned} 2^{2(2n+1)} + 1 &= (2^{2n+1} + 1)^2 - (2^{n+1})^2 \\ &= (2^{2n+1} + 2^{n+1} + 1)(2^{2n+1} - 2^{n+1} + 1). \end{aligned}$$

for $n = 14$ (our case being $n = 15$).