Short Proof of GCD($a^m + 1, a^n + 1$)

Benjamin Chen

May 28, 2024

1 Original Proof

This is a reproduction of the proof of E3288 by Kee-Wai Lau on The American Mathematical Monthly Vol. 97, No. 4 (Apr., 1990), pp. 344-345 (2 pages).

We would like to determine $\gcd(a^m + 1, a^n + 1)$.

First, let 2^i and 2^j be the largest number dividing m and n separately. i and j are the highest exponent of 2 here.

We claim that

$$d = \gcd(a^m + 1, a^n + 1) = \begin{cases} a^{\gcd(m,n)} + 1, & i = j \\ 1, & i \neq j \text{ and } a \text{ even} \\ 2, & i \neq j \text{ and } a \text{ odd} \end{cases}$$

First, we let $b = a^{\gcd(m,n)}$, $r = m/\gcd(m,n)$, and $s = n/\gcd(m,n)$. Now, we can write $d = \gcd(a^m + 1, a^n + 1) = \gcd(b^r + 1, b^s + 1)$ with $\gcd(r, s) = 1$. Then, there exist positive integers e and f such that $|er - fs| = 1$.

If $i = j$, then $\gcd(m, n)$ contains $2^i = 2^j$. Also, by the definition of i and j, the remaining r and s must be odd. Without loss of generality, we assume that $er - fs = 1$, e is odd and f is even. Now, from $b^r \equiv b^s \equiv -1 \mod d$, we have $(b^r)^e = ud - 1$ and $(b^s)^f = vd + 1$, where u and v are integers. Thus, $ud - 1 = (vd + 1)b$. Rearrange the equation, we get $ud = vbd + b + 1$. This implies that $d \mid b + 1$. Also, since r and s are odd, we get $(b + 1) \mid (b^r + 1)$ and $(b + 1) \mid (b^s + 1)$. This implies $(b + 1) \mid d$. Hence, we have $d = b + 1$.

If $i \neq j$, then r and s have different parity. Without loss of generality, we assume that r is even and s is odd. Then, $(b^r)^s = yd - 1$ and $(b^s)^r = zd + 1$ where y and z are integers. Then, $yd - 1 = zd + 1$. It implies $d \mid 2$. Also, since $2 \mid d$ only if a is odd, the result follows.

2 Extension

Since a is arbitrary, a natural extension is to replace a by x.

We are trying to determine $\gcd(x^m + 1, x^n + 1)$ where $x^m + 1, x^n + 1 \in \mathbb{Z}[x]$.

We claim

$$d = \gcd(x^m + 1, x^n + 1) = \begin{cases} x^{\gcd(m,n)} + 1, & i = j \\ 1, & i \neq j \end{cases}$$

Let $b = x^{\gcd(m,n)}, r = m/\gcd(m,n) \in \mathbb{Z}$, and $s = n/\gcd(m,n) \in \mathbb{Z}$. Now, we can write $d = \gcd(x^m + 1, x^n + 1) = \gcd(b^r + 1, b^s + 1)$ with $\gcd(r, s) = 1$. Then, there exist positive integers e and f such that $|er - fs| = 1$.

If $i = j$, then $\gcd(m, n)$ contains $2^i = 2^j$. Also, by the definition of i and j, the remaining r and s must be odd. Without loss of generality, we assume that $er - fs = 1$, e is odd and f is even. Now, from $b^r \equiv b^s \equiv -1 \mod d$, we have $(b^r)^e = ud - 1$ and $(b^s)^f = vd + 1$, where u and v are polynomials. Thus, $ud - 1 = (vd + 1)b$. Rearrange the equation, we get $ud = vbd + b + 1$. This implies that $d \mid b + 1$. Also, since r and s are odd, we get $(b + 1) \mid (b^r + 1)$ and $(b + 1) \mid (b^s + 1)$. This implies $(b + 1) \mid d$. Hence, we have $d = b + 1$.

If $i \neq j$, then r and s have different parity. Without loss of generality, we assume that r is even and s is odd. Then, $(b^r)^s = yd - 1$ and $(b^s)^r = zd + 1$ where y and z are polynomials. Then, $yd - 1 = zd + 1$. It implies $d \mid 2$. Since the polynomials are both primitive, hence, d can only be 1.