

Problem. Determine all pairs (a, b) of positive integers for which there exist positive integers g and N such that

$$\gcd(a^n + b, b^n + a) = g$$

holds for all integers $n \geq N$.

After trying to solve the problem on your own, you can find a possible solution on the next page.

Problem. Determine all pairs (a, b) of positive integers for which there exist positive integers g and N such that

$$\gcd(a^n + b, b^n + a) = g$$

holds for all integers $n \geq N$.

Proof. Let k be a positive integer and take $n = k \cdot \varphi(ab + 1) - 1$, where φ is the Euler's totient function¹. We know $x^{\varphi(ab+1)} \equiv 1 \pmod{ab+1}$ for x relatively prime to $ab+1$. Since $\gcd(ab+1, a) = 1$, we have

$$a^n + b \equiv \frac{1}{a} + b \equiv \frac{1}{a}(1 + ab) \equiv 0 \pmod{ab+1}.$$

So, $ab+1 \mid a^n + b$ and in the same way $ab+1 \mid a + b^n$. Since k is arbitrary, we can choose k large enough such that $n \geq N$. Hence, $ab+1 \mid g$. Taking $n > N$ with $n \equiv 0 \pmod{\varphi(ab+1)}$, we have

$$0 \equiv a^n + b \equiv 1 + b \pmod{ab+1}.$$

Since a and b are positive, we have $0 < 1 + b \leq 1 + ab$ and thus $1 + b = 1 + ab$, which implies $a = 1$. In the same way $b = 1$. So $a = b = 1$ is the only possible solution, which can be easily checked to work. q.e.d.

Remark 1. You can motivate the consideration of $ab+1$ as follows: We are interested in finding prime divisors p of g . The trivial ones are all of the divisors of $\gcd(a, b)$. One might work with only them for a while, but it is unclear how to finish only with these prime divisors. So, a reasonable next approach is to find prime divisors of g that are coprime to $\gcd(a, b)$. These prime factors are coprime to a and b as well.

For $p \mid g$ and p coprime to a and b , we get $p \mid b^{n-1}(a^n + b) - b^n - a = a((ab)^{n-1} - 1) = a(ab-1)((ab)^{n-2} + (ab)^{n-3} + \dots + 1)$. We can try to consider a prime divisor q of $ab-1$ in hope that q also divides $a^n + b$. This seems to be a promising approach because $ab-1$ is symmetric in a and b , coprime to a and b and no longer dependent on n . We get $a^n + b \equiv a^n + a^{-1} \equiv (a^{n+1} + 1) \frac{1}{a} \pmod{ab-1}$. So, if we can choose n in such a way that $a^{n+1} \equiv -1 \pmod{ab-1}$, it would be perfect. Unfortunately, this is not always possible. But it is possible as we make the small fix by taking $+1$ instead of -1 on the right hand side. This brings us to the consideration of $ab+1$.

One can also try considering the factor $((ab)^{n-2} + (ab)^{n-3} + \dots + 1)$ because it is symmetric in a and b and coprime to a and b . For n even, it is divisible by $ab+1$.

Remark 2. Another good approach for this problem is to consider small cases for a and b and look for common prime factors of $a^n + b$ and $b^n + a$. Then one can realize that some of them divide $ab+1$.

Plugging in $n = -1$ gives $a^n + b = \frac{1}{a} + b = \frac{1+ab}{a}$, which can also lead to the consideration of $ab+1$.

¹<https://calimath.org/wiki/eulers-totient-function>