On a Number Theory Problem: Chasing a Red Herring

Titu Andreescu & Marian Tetiva

1. Introduction: stating the problem. We all know that any two consecutive integers n and $n+1$ are relatively prime, which can also be expressed as $\gcd(n, n+1) = 1$ for any integer n. (Here and further throughout this note by $\gcd(x, y)$ we denote the greatest common divisor of the integers x and y. We have that x and y are relatively prime if and only if $\gcd(x, y) = 1$.) This is because any common divisor of n and $n+1$ must also divide $(n+1) - n = 1$. Similarly, any two consecutive odd numbers are relatively prime, that is, $\gcd(2n-1, 2n+1) = 1$ for any integer n, since any common divisor of $2n-1$ and $2n+1$ must divide their difference, which is 2. But both $2n-1$ and $2n+1$ are odd, hence the conclusion follows. We invite the reader to show similarly that $\gcd(2n+1, 4n+1) = 1$, or $\gcd(30n+3, 24n+2) = 1$ for all n. On the other hand, we evidently do not have $\gcd(2n+3, 3n+2) = 1$ for every integer n, as long as this does not hold for (at least) $n = 1$. So, naturally, we asked ourselves about the following

Problem 1. Let a, b, c, and d be integers. What necessary and sufficient conditions must they satisfy in order to have $\gcd(an+b, cn+d) = 1$ for all integers n?

The very simple (but, as we will see, also very useful to solving our problem) identity

$$a(cn+d) - c(an+b) = ad - bc$$

immediately shows that $\gcd(an+b, cn+d) = 1$ holds for all n whenever $ad - bc$ is either 1, or -1. Nevertheless, it is naive to believe that this can be a necessary and sufficient condition as long as we have a very simple example such as $\gcd(2n+1, 4n+1) = 1$ (where $a = 2$, $b = 1$, $c = 4$, $d = 1$, therefore $ad - bc = -2$). (Although many examples belong to this particular situation.) The above identity also shows that $\gcd(an+b, cn+d) = 1$ for all n whenever $ad - bc$ is nonzero and divides both a and c, since we then can rewrite it in the form

$$\frac{a}{ad-bc}(cn+d) - \frac{c}{ad-bc}(an+b) = 1,$$

with integer coefficients for $an+b$ and $cn+d$. Although many particular examples can be framed here, we see that $\gcd(30n+3, 24n+2) = 1$, or $\gcd(2n+17, 4n+66) = 1$ do not belong to this case. So, until now, we found nothing.

2. We did not find Problem 1 in the literature, although we are pretty sure that it has been studied and solved, possibly in much more general forms, so we tried to find a solution. (We mention that writing this note is not at all based on any ambition of originality. We rather intended to show how one finds a path to solving a problem through the maze of already known results, sometimes wondering and getting lost on undesired and nowhere leading trails.) We actually started from the following contest item.

Problem 2. Find all integers k for which $\gcd(4n+1, kn+1) = 1$ for all integers n.

Solution. If $d_1 = \gcd(4n+1, kn+1)$, we have (of course) that $d_1 \mid 4n+1$, and also

$$d_1 \mid k - 4 = k(4n+1) - 4(kn+1),$$

therefore

$$d_1 \mid d_2 = \gcd(4n+1, k-4).$$

But $d_2 \mid 4n+1$, too, and

$$d_2 \mid kn+1 = n(k-4) + 4n+1$$

hence $d_2 \mid d_1$. It follows that $d_1 = d_2$, implying

$$\gcd(4n+1, kn+1) = 1 \Leftrightarrow \gcd(4n+1, k-4) = 1$$

for every integer n. Thus the condition from the statement of the problem is equivalent to $\gcd(4n+1, k-4) = 1$ for all integers n. This is true if $k - 4 = \pm 2^s$ for some nonnegative integer s and some choice of the signs plus/minus, because $4n+1$ is odd and has no common factors (other than 1 and -1) with $\pm 2^s$. On the other hand, if $k-4$ has an odd factor greater than 1, that factor will be a common factor for $k-4$ and $4n+1$ for some n (this is clear if the odd factor is of the form $4t+1$; when it is of the form $4t-1$, it will be also a factor of $(4t-1)^2 = 4t(t-1)+1$). Since, under this assumption, $k-4$ and $4n+1$ cannot be relatively prime for all n, it follows that an odd factor greater than 1 is not allowed for $k-4$, and we conclude that the numbers required by the problem are those of the form 4 ± 2^s, s being a nonnegative integer.

This still doesn't suggest any general necessary and sufficient condition as required by Problem 1, but it makes a connection between $\gcd(an+b, cn+d)$ and $\gcd(cn+d, ad-bc)$ which, at first glance, seemed to us to be true in general (but is not). Namely, because

$$a(cn+d) - c(an+b) = ad - bc$$

it follows that

$$\gcd(an+b, cn+d) \mid \gcd(cn+d, ad-bc)$$

for all n. On the other hand, we also have the equality

$$n(ad-bc) + b(cn+d) = d(an+b)$$

showing that the greatest common divisor of $cn+d$ and $ad-bc$ also divides $d(an+b)$ – so, if we had $d = 1$ (as in the previous example), then

$$\gcd(cn+d, ad-bc) \mid \gcd(an+b, cn+d)$$

and, hence,

$$\gcd(cn+d, ad-bc) = \gcd(an+b, cn+d)$$

would follow.

(Similarly, when $b = 1$, $\gcd(an+b, ad-bc) = \gcd(an+b, cn+d)$ holds.) Thus we considered the case $d = 1$, and got the next result.

Problem 3. Let a, b, and c be integers. Then we have

$$\gcd(an+b, cn+1) = 1$$

for every integer n if and only if any prime divisor of $a - bc$ is also a factor of c.

Solution. As we just seen, the equality

$$a(cn+1) - c(an+b) = a - bc$$

implies

$$\gcd(an+b, cn+1) \mid \gcd(cn+1, a-bc),$$

while

$$n(a-bc) + b(cn+1) = an+b$$

implies

$$\gcd(cn+1, a-bc) \mid \gcd(an+b, cn+1)$$

so we actually get

$$\gcd(cn+1, a-bc) = \gcd(an+b, cn+1)$$

for all n. Thus we have

$$\gcd(an+b, cn+1) = 1, \ \forall\ n \in \mathbb{Z}$$
$$\Leftrightarrow \gcd(cn+1, a-bc) = 1, \ \forall\ n \in \mathbb{Z}.$$

Then it is very easy to see that the condition "any prime divisor of $a-bc$ is also a factor of c" is sufficient to have $\gcd(an+b, cn+1) = 1$, or, equivalently, $\gcd(cn+1, a-bc) = 1$ for all n. Indeed, if there exists some integer n for which $\gcd(cn+1, a-bc) > 1$, then a common prime divisor p exists for both $cn+1$ and $a-bc$. Since we assumed that $p \mid a-bc \Rightarrow p \mid c$, this p would divide both c and $cn+1$, which is impossible, so no n exists with $\gcd(an+b, cn+1) > 1$.

The condition "any prime divisor of $a-bc$ is also a factor of c" is also necessary to have $\gcd(cn+1, a-bc) = 1$ for all n. If not, we would have $\gcd(cn+1, a-bc) = 1$ for all n, while a prime q would exist such that $q \mid cn+1$, and q does not divide c. But, this being the case, we can find an n such that $cn+1 \equiv 0 \mod q$ (the congruence $cx+1 \equiv 0 \mod q$ is solvable). Since q also divides $a-bc$, we get the contradiction $q \mid \gcd(cn+1, a-bc)$, thus finishing the proof.

Well, this was the *red herring* that troubled our way towards the demonstration for the general case: the misleading idea that we could use a connection between $\gcd(an+b, cn+d)$ and $\gcd(cn+d, ad-bc)$ (or $\gcd(an+b, ad-bc)$), as we did in the previous Problems 2 and 3. Nevertheless, Problem 3 (and its particular case, Problem 2) finally led us to the general necessary and sufficient conditions for which Problem 1 asks (but only when we decided to give up chasing chimeras). Observing that "any prime divisor of $a-bc$ is also a factor of c" implies "any prime divisor of $a-bc$ is also a factor of a", too (and, anyway, some symmetry about a and c is inevitable) we finally realized what we were looking for.

3. The solution. We now solve Problem 1, after we reformulate it as

Problem 4. For integers a, b, c, d the following statements are equivalent.

(i) The numbers $an+b$ and $cn+d$ are relatively prime for any integer n.

(ii) We have that b and d are relatively prime, and any prime divisor of $ad-bc$ is also a factor of both a and c.

Solution. The condition $\gcd(b, d) = 1$ is obviously necessary in order to have $\gcd(an+b, cn+d) = 1$ for any integer n (take $n = 0$) – and we assume further that this is the case. Then note that the equality

$$a(cn+d) - c(an+b) = ad - bc$$

holds for any n, and assume that a prime p divides $ad-bc$, but it does not divide a. Since a is relatively prime to p, the congruence $ax+b \equiv 0 \mod p$ is solvable, hence we can find an integer n satisfying it, that is, such that

$$an+b \equiv 0 \mod p.$$

Multiplying this by d, and using the divisibility of $ad-bc$ by p, we get

$$bcn + bd \equiv adn + bd \equiv 0 \mod p,$$

or

$$b(cn+d) \equiv 0 \mod p.$$

Now, if p divides b, since it also divides $ad-bc$, it follows that p divides ad. But p does not divide a, hence we get $p \mid d$, and the assumption that b and d are relatively prime is contradicted. So p does not divide b, hence $b(cn+d) \equiv 0 \mod p$ implies $cn+d \equiv 0 \mod p$. We summarize: when $\gcd(b, d) = 1$, if a prime p exists such that p divides $ad-bc$, but p does not divide a, then we can find an integer n such that $\gcd(an+b, cn+d) > 1$ (p divides both $an+b$ and $cn+d$). Similarly, the existence of a prime that divides $ad-bc$, but it does not divide c leads to the same conclusion. Thus, for $\gcd(an+b, cn+d) = 1$ to hold for all integers n it is necessary to have $\gcd(b,d) = 1$, and, also, to have that any prime factor of $ad-bc$ is a prime factor of both a and c.

Now we show that these two conditions are also sufficient in order to have $\gcd(an+b, cn+d) = 1$ for all n. That is, we assume that $\gcd(b,d) = 1$, and that any prime dividing $ad-bc$ also divides both a and c, and we show that $\gcd(an+b, cn+d) = 1$ for all n.

Indeed, let q be a common prime factor of $an+b$ and $cn+d$, for some integer n. By using again the identity

$$a(cn+d) - c(an+b) = ad - bc$$

we see that q divides $ad-bc$. But then, by hypothesis, q divides a, and q divides c, hence q divides $b = (an+b) - an$, and q divides $d = (cn+d) - cn$. This comes in contradiction with the hypothesis $cd(b,d) = 1$, hence the assumption that a prime common factor exists for $an+b$ and $cn+d$ (for some n) is false, and the desired conclusion $\gcd(an+b, cn+d) = 1$ for any integer n follows.

4. Final remarks. Note that, by contraposition, we get the next rewording of our main result (Problem 4):

Problem 4′. For integers a, b, c, d the following statements are equivalent.

(i) There exists an integer n such that $an+b$ and $cn+d$ are not relatively prime.

(ii) We either have $\gcd(b,d) > 1$, or there exists a prime divisor of $ad-bc$ that does not divide either a, or c.

Also, note some particular cases of the main result.

- In Problem 2 we have $a = 4$, $b = 1$, $c = k$, and $d = 1$, therefore the condition $\gcd(b,d) = 1$ is fulfilled. Since $ad - bc = 4 - k$, by the result of Problem 4, for $\gcd(4n+1, kn+1) = 1$ to hold it is necessary and sufficient that any prime factor of $4-k$ is also a factor of 4 and of k. This means $4 - k = \pm 2^s$, hence $k = 4 \pm 2^s$ for some nonnegative integer s, and if this is the case, 2 (the only prime factor of $ad - bc = 4k$) is, indeed, a factor of not only 4, but of k too. The result (as proved above) follows.

- When $ad - bc = 1$, or $ad - bc = -1$ the conditions $\gcd(b,d) = 1$ and $p \mid ad - bc \Rightarrow p \mid a$ and $p \mid c$ (for a prime p) are automatically satisfied (the second because no prime divisor of $ad - bc$ exists), hence $\gcd(an+b, cn+d) = 1$ follows for any integer n. Slightly more generally, if $\gcd(b,d) = 1$, $ad - bc \mid a$, and $ad - bc \mid c$, then $\gcd(an+b, cn+d) = 1$ for any n.

  (Again, the equality $a(cn+d) - c(an+b) = ad - bc$ immediately implies these results.) Most of the usual examples one meets in elementary arithmetics textbooks, such as $\gcd(n, n+1) = 1$, $\gcd(n+1, 2n+1) = 1$, or $\gcd(2n+1, 4n+1) = 1$ belong to one of these two particular cases – which we also discussed in the Introduction. (Nevertheless, there also exist situations that do not fit into these cases: for – one more – example, we have $\gcd(6n+5, 12n+6) = 1$ for all n.)

- Also, observe that when $ad - bc = 0$, we have $\gcd(an+b, cn+d) = 1$ for any n if and only if $a = c = 0$ and $\gcd(b,d) = 1$.

- If we have $a = c = 1$ the condition ”any prime dividing $ad - bc$ also divides both a and c” can only be fulfilled for $ad - bc = 1$, or $ad - bc = -1$, meaning that $d - b \in \{1, -1\}$. This closes a circle, since it leads us to the very first (and simplest, and most known) example we gave: any two consecutive integers are relatively prime.

Finally, we invite the reader to see that $2n+1$ and $4n-17$ are not relatively prime for any n, and to find such an n that $2n+1$ and $4n-17$ have a common divisor greater than 1.