Contents

Preface

This is a collection of articles written by the coordinating author and many dear friends. We arranged the articles in a book for math lovers involved in competitions and anyone interested in expanding their mathematical horizons. In terms of level, they range from intermediate to advanced. The articles delve into several branches of mathematics such as algebra, geometry, combinatorics, and number theory—precisely those realms of the queen of sciences that are subject to the International Mathematical Olympiad and also mathematical analysis. Thus we have in this book articles treating some elementary (and somehow unusual) inequalities (both algebraic and geometric), in particular one article that cleverly uses the Cauchy-Schwarz inequality for solving a difficult number theory problem. Speaking of number theory, one can find in the book topics such as Diophantine equations, the Ramanujan sums, Kronecker's and Weyl's density theorems, and the distribution of consecutive integers divisible by their number of divisors. In geometry, the Malfatti problem, Newton's theorem about circumscriptible quadrilaterals, Napoleon polygons, and equifacial tetrahedra are examined. Cayley's theorem about the number of spanning trees of the complete graph on n vertices, functional equations, and two articles that start from some old Romanian team selection test problems and get into higher algebra and mathematical analysis complete this book which, we think and we hope, will be of interest for the (more or less) young lovers of mathematics. We invite them all to carefully read and, consequently, enjoy the beautiful mathematical landscapes that we offer—exactly because we believe in the power of the magnificent beauty of mathematics.

1 On a Class of Sums Involving the Floor Function

Titu Andreescu and Dorin Andrica

For a real number x, there is a unique integer n such that $n \leq x < n+1$. We say that n is the *greatest integer less than or equal to* x or the *floor of* x and is denoted by $\lfloor x \rfloor$. The difference $x - \lfloor x \rfloor$ is called the *fractional part of* x and is denoted by $\{x\}$.
The least integer greater than or equal to x is called the *ceiling of* x and is denoted by $\lceil x \rceil$.
The following properties are useful.
1. If a and b are integers, $b > 0$, and q is the quotient when a is divided by b, then $q = \left\lfloor \frac{a}{b} \right\rfloor$.
2. For any real number x and any integer n, $\lfloor x+n \rfloor = \lfloor x \rfloor + n$ and $\lceil x+n \rceil = \lceil x \rceil + n$.
3. For any positive real number x and any positive integer n, the number of positive multiples of n not exceeding x is $\left\lfloor \frac{x}{n} \right\rfloor$.
4. For any real number x and any positive integer n, $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor$.
We will prove the last two properties. For 3) consider all multiples $1 \cdot n$, $2 \cdot n, \ldots, k \cdot n$, where $k \cdot n \leq x < (k+1)n$. That is, $k \leq \frac{x}{n} < k+1$, and the conclusion follows. For 4) let $\lfloor x \rfloor = m$ and $\{x\} = \alpha$. By the division algorithm and property 1) above, it follows that $m = n \left\lfloor \frac{m}{n} \right\rfloor + r$, where $0 \leq r \leq n-1$. We obtain $0 \leq r + \alpha \leq n - 1 + \alpha < n$; that is, $\left\lfloor \frac{r+\alpha}{n} \right\rfloor = 0$ and

$$\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{m+\alpha}{n} \right\rfloor = \left\lfloor \left\lfloor \frac{m}{n} \right\rfloor + \frac{r+\alpha}{n} \right\rfloor = \left\lfloor \frac{m}{n} \right\rfloor + \left\lfloor \frac{r+\alpha}{n} \right\rfloor$$
$$= \left\lfloor \frac{m}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor.$$

The following result is helpful in proving many relations involving the floor function.

Theorem 1. *Let p be an odd prime and let q be an integer that is not divisible by p. If $f : \mathbb{Z}_+ \to \mathbb{R}$ is a function such that:*
(i) $\dfrac{qf(k)}{p}$ is not an integer, $k = 1, 2, \ldots, p-1$;
(ii) $f(k) + f(p-k)$ is an integer divisible by p, $k = 1, 2, \ldots, p-1$, then

$$\sum_{k=1}^{p-1} \left\lfloor f(k)\frac{q}{p} \right\rfloor = \left(\frac{q}{p} \sum_{k=1}^{p-1} f(k) \right) - \frac{p-1}{2}. \tag{1}$$

Proof. From (ii) it follows that

$$\frac{qf(k)}{p} + \frac{qf(p-k)}{p} \in \mathbb{Z} \tag{2}$$

and from (i) we obtain that $\dfrac{qf(k)}{p} \notin \mathbb{Z}$ and $\dfrac{qf(p-k)}{p} \notin \mathbb{Z}$, $k=1, \ldots, p-1$. Hence

$$0 < \left\{ \frac{qf(k)}{p} \right\} + \left\{ \frac{qf(p-k)}{p} \right\} < 2.$$

But, from (1), $\left\{ \dfrac{qf(k)}{p} \right\} + \left\{ \dfrac{qf(p-k)}{p} \right\} \in \mathbb{Z}$, thus

$$\left\{ \frac{qf(k)}{p} \right\} + \left\{ \frac{qf(p-k)}{p} \right\} = 1, \quad k = 1, \ldots, p-1.$$

Summing over all k and dividing by 2 gives

$$\sum_{k=1}^{p-1} \left\{ \frac{q}{p} f(k) \right\} = \frac{p-1}{2}.$$

It follows that

$$\sum_{k=1}^{p-1} \frac{q}{p} f(k) - \sum_{k=1}^{p-1} \left\lfloor \frac{q}{p} f(k) \right\rfloor = \frac{p-1}{2},$$

and the conclusion follows.

Application 1. The function $f(x) = x$ satisfies (i) and (ii) in Theorem 1. Hence

$$\sum_{k=1}^{p-1} \left\lfloor k \cdot \frac{q}{p} \right\rfloor = \frac{q}{p} \cdot \frac{(p-1)p}{2} - \frac{p-1}{2},$$

that is,

$$\sum_{k=1}^{p-1} \left\lfloor k \cdot \frac{q}{p} \right\rfloor = \frac{(p-1)(q-1)}{2} \quad \text{(Gauss)}. \tag{3}$$

Remark 1. From the proof of our Theorem, it follows that the above formula holds for any relatively prime integers p and q.

Application 2. The function $f(x) = x^3$ satisfies (i) and (ii) in Theorem 1.

Hence

$$\sum_{k=1}^{p-1} \left\lfloor k^3 \cdot \frac{q}{p} \right\rfloor = \frac{q}{p} \cdot \frac{(p-1)^2 p^2}{4} - \frac{p-1}{2} = \frac{(p-1)(p^2 q - pq - 2)}{4}. \tag{4}$$

For $q = 1$, we obtain the 2002 German Mathematical Olympiad problem:

$$\sum_{k=1}^{p-1} \left\lfloor \frac{k^3}{p} \right\rfloor = \frac{(p-2)(p-1)(p+1)}{4}. \tag{5}$$

Application 3. For $f : \mathbb{Z}_+ \to \mathbb{R}$, $f(s) = (-1)^s s^2$, conditions (i) and (ii) in Theorem 1 are both satisfied. We obtain

$$\begin{aligned} \sum_{k=1}^{p-1} \left\lfloor (-1)^k k^2 \cdot \frac{q}{p} \right\rfloor &= \frac{q}{p}(-1^2 + 2^2 - \cdots + (p-1)^2) - \frac{p-1}{2} \\ &= \frac{q}{p} \cdot \frac{p(p-1)}{2} - \frac{p-1}{2}. \end{aligned}$$

Hence

$$\sum_{k=1}^{p-1} \left\lfloor (-1)^k k^2 \cdot \frac{q}{p} \right\rfloor = \frac{(p-1)(q-1)}{2}. \tag{6}$$

Application 4. By taking $q = 1$ we get

$$\sum_{k=1}^{p-1} \left\lfloor (-1)^k \frac{k^2}{p} \right\rfloor = 0.$$

Using the identity $\lfloor -x \rfloor = 1 - \lfloor x \rfloor$ for $x \in \mathbb{R} - \mathbb{Z}$, the last equality takes the form

$$\sum_{k=1}^{p-1} (-1)^k \left\lfloor \frac{k^2}{p} \right\rfloor = \frac{p-1}{2}. \tag{7}$$

Application 5. Similarly, applying Theorem 1 to $f : \mathbb{Z}_+ \to \mathbb{R}$,

$$f(s) = (-1)^s s^4$$

yields

$$\sum_{k=1}^{p-1} \left\lfloor (-1)^k k^4 \cdot \frac{q}{p} \right\rfloor = \frac{q(p-1)(p^2-p-1)}{2} - \frac{p-1}{2}. \tag{8}$$

Taking $q = 1$ gives

$$\sum_{k=1}^{p-1} \left\lfloor (-1)^k \cdot \frac{k^4}{p} \right\rfloor = \frac{(p-2)(p-1)(p+1)}{2}. \tag{9}$$

Application 6. For $f(s) = \dfrac{s^p}{p}$, conditions (i) and (ii) in Theorem 1 are also satisfied.
For $q = 1$ we obtain

$$\sum_{k=1}^{p-1} \left\lfloor \frac{k^p}{p^2} \right\rfloor = \frac{1}{p} \sum_{k=1}^{p-1} \frac{k^p}{p} - \frac{p-1}{2} = \frac{1}{p^2} \left(\sum_{k=1}^{p-1} k^p - \frac{p(p-1)}{2} \right),$$

hence

$$\sum_{k=1}^{p-1} \left\lfloor \frac{k^p}{p^2} \right\rfloor = \frac{1}{2} \sum_{k=1}^{p-1} \frac{k^p - k}{p}. \tag{10}$$

Formula (10) shows that half of the sum of quotients obtained when $k^p - k$ is divided by p (Fermat's little theorem) is equal to the sum of the quotients obtained when k^p is divided by p^2, $k = 1, 2, \ldots, p-1$.

Bibliography

[1] T. Andreescu, D. Andrica, *Number Theory and its Mathematical Structures,* Birkhäuser, Boston–Basel–Berlin.

Originally published in Mathematical Reflections, 5(2006)

2 On a Number Theory Problem: Chasing a Red Herring

Titu Andreescu and 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, $\gcd(x, y)$ denotes 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 $\gcd(2n+1, 4n+1) = 1$ and $\gcd(30n+3, 24n+2) = 1$ 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 naïve 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 $\gcd(30n+3, 24n+2)=1$ and $\gcd(2n+17, 4n+66)=1$ do not belong to this case. So, until now, we've 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 problem.

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 obtained 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 have 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

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

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 $cn+1 \equiv 0 \pmod{q}$ (i.e., the congruence $cx+1 \equiv 0 \pmod{q}$ 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 $ax+b\equiv 0 \pmod{p}$ is solvable, hence we can find an integer n satisfying it, that is, such that

$$an+b\equiv 0 \pmod{p}.$$

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

$$bcn+bd\equiv adn+bd\equiv 0 \pmod{p},$$

or

$$b(cn+d)\equiv 0 \pmod{p}.$$

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 $b(cn+d)\equiv 0 \pmod{p}$ implies $cn+d\equiv 0 \pmod{p}$. 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 $\gcd(an+b, cn+d)>1$