FORWARD

PREDA MIHĂILESCU

Exercises are in mathematics like a vitalizer: they strengthen and train the elasticity of the mind, teach a variety of successful methods for approaching specific problems, and enrich the professional culture with interesting questions and results. For a good treatment of a theory, examples and exercises are the art of presenting concrete applications, reflecting the strength and potential of the theoretical results. A strong theory explained only by simple exercise often may reduce the motivation of the reader.

At the other end, there is a wide reserve of problems and exercises of elementary looking nature, but requiring vivid mind and familiarity with a good *bag of tricks*, problems of styles which were much developed by the interest that mathematical competition attracted worldwide in the last 50 years. These problems can only loosely be ordered into applications of individual theories of mathematics, their flavor and interest relaying in the way they combine different areas of knowledge with astute techniques of solving. Often, not always, the problems addressed have some deeper interest of their own and can very well be encountered as intermediate steps in the development of mathematical theories. From this perspective, a good culture of problems can be to a mathematician as helpful, as the familiarity with classical situations in chess matches, to a professional chess player: they develop the aptitude to recognize, formulate and solve individual problems that may play a crucial role in theories and proofs of deeper significance.

The book at hand is a powerful collection of competition problems with number theoretical flavor. They are generally grouped according to common aspects, related to topics like *Divisibility, GCD and LCM, decomposition of polynomials, Congruences and p-adic valuations*, etc. And these aspects can be found in the problems discussed in the respective chapter – beware though to expect much connection to the typical questions one would find in an introductory textbook to number theory, at the chapters with the same name. The problems here are innovative findings and questions, and the connection is more often given by the methods used for the solution, than by the very nature of the problem.

Some problems have a simple combinatorial charm of their own, without requiring much more than good observation – for instance (p. 512, N 25), *Find all* $m, n, p \in \mathbf{Q}_{>0}$ *such that all of the numbers* $m + \frac{1}{np}$, $n + \frac{1}{pm}$, $p + \frac{1}{mn}$ *are integers*. Others appear even weird at a first glance, like (p. 656, N 8): *For coprime positive integers* p, q, *prove that:*

$$\sum_{k=0}^{pq-1} (-1)^{\lfloor k/p \rfloor + \lfloor k/q \rfloor} = \begin{cases} 0 & \text{if } pq \text{ is even} \\ 1 & \text{if } pq \text{ is odd} \end{cases};$$

or (N 36, p. 543), requiring to show that infinitely many primes are coprime to the terms of the polynomially recursive sequence given by $a_1 = 1$ and $a_{n+1} = (a_n^2 + 1)^2 - a_n^3$. When one then does the homework, one notices that several useful and non trivial notions about floors are required for solving the problem.

The book also contains some basic propositions, which are in big part classical theorems, but also more specialized results, that can be applied for solving further problems. Thus, beyond the spontaneous charm of some of the exercises, most problems are involved and require a good combination of solid understanding of the theoretical basics, with a good experience in problem solving.

Working through the book one learns a lot. Do you want to know more on how large the difference between the product of k consecutive integers and their LCM can become? A series of results will provide an answer – and you will then certainly find also a set of variations of this theme. For primes p, the Fermat quotient $\phi(2) = \frac{2^{p-1}-1}{p} \mod p$ has a well known development in terms of harmonic sums. But if you want to know higher terms in its p-adic development, you can find them in the chapter on p-adic values. Together with a series of less known, classical congruences of higher order of Wolfenstone, Morley, Ljunggren et. al., this leads to a series of interesting questions and problems.

Not all problems are atomic training subjects; at the contrary, by a good choice of the problems, the authors may group elementary results that lead to remarkable understanding of some fundamental number theoretical functions, like π, σ, τ, ϕ – the prime distribution function, the number of divisors and their sum, and the Euler totient, respectively. Here also, if you want for instance to

understand how it happens that the fibers of the inverse $\phi^{-1}(X)$ of the Euler totient may become indefinitely large, several exercises lead to the understanding of this phenomenon. It will not surprise that among the authors or solvers of the problems presented, one encounters numerous famous mathematicians, from classical to contemporaneous, ranging from Gauss, Lagrange, Euler and Legendre, through V. Lebesgue, Lucas, but also Hurwitz and, unsurprisingly, Erdős and Schinzel: the borders between research mathematics and advanced problem solving are fluid.

This very short and selective overview of the book should have already suggested that the book can be read with various attitudes and expectations, and there is always much to profit from it. The reader may traverse entire chapters of the book and get familiar with the specifics of the posed problems, but should definitely invest the time for trying to solve at least two or three problems alone, each time when working again with this book. In spite of the well structured construction of the book, one can easily jump to chapters or sections of interest – they are to a large extent self-consistent. And if not, good references help to find the necessary facts which were discussed at previous places of the book.

Altogether – while students eager to acquire experience helping to reach outstanding performance in mathematical competitions will profit most from this book, it is certainly a good companion both for professional mathematicians and for any adult with an active interest in mathematics Each one of them will find it a leisure to read and work over and over again through the problems of this book.

Preda Mihăilescu
Göttingen, May 2017
Mathematisches Institut der Universität Göttingen
E-mail: preda@uni-math.gwdg.de

Contents

Chapter 1

Introduction

Based on lectures given by the authors at the AwesomeMath Summer Program over several years, this book is a slightly non-standard introduction to elementary number theory. Nevertheless, it still develops theoretical concepts from scratch with full proofs. The book insists on exemplifying these results through interesting and rather challenging problems. In particular, the reader will not find many advanced concepts in this book, but will encounter quite a lot of intriguing results that can be proven using "basic" number theory yet nonetheless test one's problem-solving aptitude.

The book is divided into six large chapters, each focusing on a fundamental concept or result. Each chapter is itself divided into sections that reinforce a specific topic through a large series of examples arranged (subjectively) in increasing order of difficulty. In particular, the first two chapters are largely elementary but fundamental for appreciating the rest of the book. The topics explored in these two chapters are classical: divisibility, congruences, Euclidean division, greatest common divisor, and least common multiple. With the theoretical concepts being fairly elementary, the focus is more on concrete problems and interesting applications, for instance, Diophantine equations, finite differences, and problems with a combinatorial flavor. The third chapter is devoted to the fundamental theorem of arithmetic and its numerous applications. After proving basic properties of prime numbers and the uniqueness of prime factorization, the authors emphasize their utility and vast scope among

arithmetic functions. There are many non-standard and sometimes surprising results in this chapter.

The fourth and fifth chapters, devoted to congruences involving prime numbers and to the distribution of prime numbers, are in some sense the heart of the book. Each of the classical congruences (Fermat, Wilson, Lagrange, and Lucas) is studied in depth in the fourth chapter, along with numerous examples of their use, for instance, quadratic residues, the number of solutions to polynomial congruences, and congruences involving binomial coefficients or higher congruences. In the fifth chapter, p-adic valuations are used to study the distribution of prime numbers. This has the advantage of being fairly elementary, while still producing beautiful and nontrivial results. The key results of this chapter are Legendre's theorem and the arithmetic of binomial coefficients, leading to strong results concerning the distribution of prime numbers. Finally, the sixth chapter discusses congruences for composite moduli, introducing further essential concepts and results: the Chinese remainder theorem, Euler's theorem, and their applications to primitive roots modulo integers. The main focus is again providing many examples of these concepts' applications (in particular, the reader will find a whole section devoted to systems of congruences). Each chapter contains a long list of practice problems, whose solutions are presented at the end of the book.

Experience has shown that it is easier to make students appreciate the beauty and power of a result when it is enhanced by pertinent and challenging examples. We strove to achieve this, a possible explanation for the book's length, although the theoretical material is rather classical and standard.

We would like to thank our students at the AwesomeMath Summer Program on whom we tested a large part of this material and who supplied many of the solutions presented here. We are also indebted to Richard Stong for a very careful reading of the book, for pointing out many inaccuracies, and for supplying a great deal of solutions (many of which were simpler and more elegant than ours!).

Titu Andreescu Gabriel Dospinescu Oleg Mushkarov

Chapter 2

Divisibility

This first chapter is fairly elementary and discusses basic properties of divisibility, congruences and the Euclidean division. These will be constantly used later on in the book and represent the foundations of arithmetic, on which we will build more advanced results later on. We tried to insist more on relatively nonstandard examples or applications, some of which are relatively nontrivial (such as the topic of finite differences and their applications to congruences).

2.1 Basic properties

In this section we introduce the notion of divisibility and study some of its basic properties.

2.1.1 Divisibility and congruences

We start by defining the divisibility relation.

Definition 2.1. Let a, b be integers. We say that a divides b and write $a \mid b$ if there is an integer c such that $b = ac$.

There are many equivalent ways of saying that a divides b: we can also say that b is divisible by a, that a is a divisor of b or that b is a multiple of a. All

these formulations are used in practice. Note that if $a \neq 0$, then saying that a divides b is equivalent to saying that the rational number $\frac{b}{a}$ is an integer. The previous definition takes into account the possibility that $a = 0$, in which case a divides b if and only if $b = 0$. In other words, any integer is a divisor of 0, and 0 is the only multiple of 0.

If 2 divides an integer n, we say that n is even. Otherwise, we say that n is odd. Thus the even integers are $..., -2, 0, 2, 4, 6, ...$, while the odd ones are $... - 3, -1, 1, 3, 5, ...$ Note that if n is odd, then $n - 1$ is even, in other words any integer n is either of the form $2k$ or $2k + 1$ for some integer k. In particular, we obtain that the product of two consecutive integers is always even. We deduce for instance that if a is an odd integer, say $a = 2k + 1$, then

$$a^2 - 1 = 4k(k + 1)$$

is a multiple of 8. In particular any perfect square (i.e. number of the form x^2 with x an integer) is either a multiple of 4 or of the form $8k + 1$ for some integer k.

The following result summarizes the basic properties of the divisibility relation.

Proposition 2.2. *The divisibility relation has the following properties:*

1. *(reflexivity) a divides a for all integers a.*
2. *(transitivity) If $a \mid b$ and $b \mid c$, then $a \mid c$.*
3. *If $a, b_1, ..., b_n$ are integers and $a \mid b_i$ for $1 \leq i \leq n$, then $a \mid b_1c_1 + ... + b_nc_n$ for all integers $c_1, ..., c_n$.*
4. *If $a \mid b$ and $a \mid b \pm c$, then $a \mid c$.*
5. *If $n \mid a - b$ and $n \mid a' - b'$, then $n \mid aa' - bb'$.*

Proof. All of these properties follow straight from the definition. We only prove properties 3) and 5) here, leaving the others to the reader. For property 3), write $b_i = ax_i$ for some integers x_i. Then

$$b_1c_1 + ... + b_nc_n = ax_1c_1 + ... + ax_nc_n = a(x_1c_1 + ... + x_nc_n)$$

is a multiple of a. For property 5), write $a-b=kn$ and $a'-b'=k'n$ for some integers k,k'. Then

$$aa'-bb'=(b+kn)(b'+k'n)-bb'=n(bk'+b'k+nkk'),$$

thus $n \mid aa'-bb'$. □

We introduce next a key notation and definition, that of congruences:

Definition 2.3. Let a,b,n be integers. We say that a and b are congruent modulo n and write

$$a \equiv b \pmod{n}$$

if $n \mid a-b$.

Most parts of the following theorem are simple reinterpretations of proposition 2.2. They are of constant use in practice.

Theorem 2.4. *For all integers a,b,c,d,n we have*

a) (reflexivity) $a \equiv a \pmod{n}$.

b) (symmetry) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.

c) (transitivity) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

d) If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a+b \equiv c+d \pmod{n}$ and $ab \equiv cd \pmod{n}$.

e) If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{nc}$. Conversely, if $ac \equiv bc \pmod{nc}$ and $c \neq 0$, then $a \equiv b \pmod{n}$.

Proof. a), b), c), d) are either clear or consequences of proposition 2.2. Property e) is immediate and left to the reader. □

Remark 2.5. We cannot cancel congruences without taking care. In other words, it is not true that if $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$ or $a \equiv 0 \pmod{n}$. For instance $2 \cdot 2 \equiv 2 \cdot 0 \pmod{4}$, but 2 is not congruent to 0 modulo 4. We will see later on that we can "cancel a" in a congruence $ab \equiv ac \pmod{n}$ provided n and a share no common divisor except ± 1.

Let us illustrate the previous theorem with some concrete problems (where no congruence is mentioned!).

Example 2.6. Find the last digit of $9^{1003} - 7^{902} + 3^{801}$.

Proof. We have $9^{1003} \equiv (-1)^{1003} \equiv -1 \equiv 9 \mod 10$. In addition,

$$7^{902} \equiv 49^{451} \equiv (-1)^{451} \equiv -1 \mod 10.$$

Finally,

$$3^{801} \equiv 3 \cdot (3^4)^{200} \equiv 3 \cdot 1^{200} \equiv 3 \mod 10.$$

Hence

$$9^{1003} - 7^{902} + 3^{801} \equiv (-1) - (-1) + 3 \equiv 3 \mod 10,$$

so the last digit is 3. □

Example 2.7. Prove that for any $n \in \mathbf{N}$ the number $a_n = 11^{n+2} + 12^{2n+1}$ is divisible by 133.

Proof. We have $12^2 = 144 \equiv 11 \pmod{133}$, hence

$$a_n \equiv 11^{n+2} + 12 \cdot 144^n \equiv 11^{n+2} + 12 \cdot 11^n \equiv 11^n(121 + 12) \equiv 0 \pmod{133}. \quad \square$$

Example 2.8. (Kvant, M 274) Find the least number of the form:
(i) $|11^k - 5^l|$,
(ii) $|36^k - 5^l|$,
(iii) $|53^k - 37^l|$,
where k and l are positive integers.

Proof. (i) The last digit of $|11^k - 5^l|$ is either 6 or 4, thus the least number of the form $|11^k - 5^l|$ must be at least 4. Since $|11^2 - 5^3| = 4$, we deduce that the answer is 4.

(ii) We have $11 = |36 - 5^2|$ and we will show that this is the least number of the form $|36^k - 5^l|$. Suppose that for some k, l we have $|36^k - 5^l| \leq 10$. Since $36^k - 5^l \equiv 6 - 5 = 1 \pmod{10}$, we deduce that $36^k - 5^l = 1$ or $36^k - 5^l = -9$. The first equality is impossible since it would imply that $0 - 1 \equiv 1 \pmod 4$, impossible. The second equality is also impossible since it would yield $0 - (-1)^l \equiv 0 \pmod 3$, again impossible. This finishes the proof.

(iii) Note first that the given numbers are divisible by 4 since 53^k and 37^l are congruent to 1 modulo 4. We will show that the desired number is $16 = |53 - 37|$. Note that

$$53^k \equiv (-1)^k \pmod 9, \quad 37^l \equiv 1 \pmod 9.$$

Hence $N = |53^k - 37^l| \equiv 0, \pm 2 \pmod 9$ which shows that $N \neq 4, 8, 12$. □

The following fundamental theorem is of constant use.

Theorem 2.9. *a) If a, b are integers, then $a - b \mid a^k - b^k$ for all $k \geq 1$.*

b) More generally, if d, n are positive integers such that $d \mid n$, then $a^d - b^d \mid a^n - b^n$ for all integers a, b. Moreover, if $\frac{n}{d}$ is odd, then $a^d + b^d \mid a^n + b^n$ for all integers a, b (in particular $a + b \mid a^n + b^n$ for all integers a, b if n is odd).

Proof. a) This follows directly from the identity

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + ... + ab^{k-2} + b^{k-1}).$$

b) Let $n = kd$ for some positive integer k. Then setting $x = a^d$, $y = b^d$ we are reduced to showing that $x - y \mid x^k - y^k$ (which follows from part a)) and $x + y \mid x^k + y^k$ when k is odd, which follows from

$$x + y = x - (-y) \mid x^k - (-y)^k = x^k + y^k.$$ □

Remark 2.10. 1) We will see later on that under rather weak hypotheses, the divisibility $a^m - b^m \mid a^n - b^n$ implies $m \mid n$.

2) The identity

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1})$$

is absolutely fundamental in arithmetic and the reader should become very familiar with it, since it will be used constantly in this book. Indeed, in many cases the results of theorem 2.9 are strong enough, but in some circumstances a finer analysis of the term $a^{n-1} + a^{n-2}b + ... + b^{n-1}$ is crucial.

The following result is a simple translation of the previous theorem in terms of congruences:

Corollary 2.11. *Let a, b, n be integers, let k be a positive integer and let $d \mid k$ a positive divisor of k.*

a) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.

b) If $a^d \equiv b^d \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.

c) If $a^d \equiv -b^d \pmod{n}$ and $\frac{k}{d}$ is odd, then $a^k \equiv -b^k \pmod{n}$.

Example 2.12. Using that $641 = 2^7 \cdot 5 + 1$, prove that $641 \mid 2^{32} + 1$.

Proof. We have $2^7 \cdot 5 \equiv -1 \pmod{641}$, thus $2^{28} \cdot 5^4 \equiv 1 \pmod{641}$. Since $641 = 5^4 + 2^4$ we have $5^4 \equiv -2^4 \pmod{641}$, thus $2^{28} \cdot 5^4 \equiv -2^{32} \pmod{641}$ and so $-2^{32} \equiv 1 \pmod{641}$, which is exactly what we need. □

Example 2.13. a) Prove that if n is a positive integer, then 9 divides the difference between n and the sum of its decimal digits.

b) Let n be a positive integer and let S_1 (respectively S_2) be the sum of the digits of n at the odd (respectively even) positions (the last digit of n has position 0). Prove that $n \equiv S_2 - S_1 \pmod{11}$.

Proof. a) Write

$$n = \overline{a_k a_{k-1} ... a_0} = a_k \cdot 10^k + a_{k-1} 10^{k-1} + ... + a_0$$

for some decimal digits $a_k, ..., a_0$ with $a_k \neq 0$. Then

$$n - (a_0 + a_1 + ... + a_k) = a_k(10^k - 1) + a_{k-1}(10^{k-1} - 1) + ... + a_1(10 - 1)$$

is a multiple of 9, since each term in the sum is a multiple of 9 thanks to theorem 2.9.

b) The proof is identical to that of part a), the key point being the congruence $10^i \equiv (-1)^i \pmod{11}$ for all i. □

Example 2.14. (Kvant M 676) Prove that for every positive integer n the sum of the digits of 1981^n is not less than 19.

Proof. Write $S(x)$ for the sum of the decimal digits of x. Since $9 \mid x - S(x)$ for all x and since $9 \mid 1981^n - 1$ (as $9 \mid 1980$), it follows that $9 \mid S(1981^n) - 1$ and so $S(1981^n)$ is one of the numbers $1, 10, 19, ...$ Since 1981^n ends in 1 (because

$10 \mid 1981^n - 1$) it follows that $S(1981^n) > 1$. Suppose that $S(1981^n) = 10$, thus $S(1981^n - 1) = 9$. Denote by S_1 (respectively S_2) the sum of the digits of $1981^n - 1$ at the odd (respectively even) positions. Then $0 \leq S_1, S_2 \leq 9$. On the other hand $1981^n - 1$ is divisible by 1980, thus it is divisible by 11. Hence $S_1 - S_2$ is divisible by 11 (by the previous example) and we conclude that $S_1 = S_2$. But $S_1 + S_2 = 9$, a contradiction.Thus $S(1981^n) \geq 19$ for all n. □

Example 2.15. Let $F_n = 2^{2^n} + 1$ be the nth Fermat number. Prove that $F_n | 2^{F_n} - 2$ for all $n \geq 1$.

Proof. It suffices to show that $F_n \mid 2^{F_n - 1} - 1$. Note that

$$F_n \mid (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1.$$

If $a \mid b$ then $2^a - 1 \mid 2^b - 1$ by theorem 2.9. It suffices therefore to show that $2^{n+1} \mid F_n - 1$, or equivalently $n + 1 \leq 2^n$. This is clear. □

An immediate consequence of the previous theorem is the following very useful:

Proposition 2.16. *If f is a polynomial with integer coefficients, then for all integers a, b*

$$a - b \mid f(a) - f(b).$$

Thus, if $a \equiv b \pmod{n}$ for some integer n, then $f(a) \equiv f(b) \pmod{n}$.

Proof. Write

$$f(X) = c_0 + c_1 X + ... + c_n X^n$$

for some integers $c_0, ..., c_n$ and some $n \geq 0$. Then

$$f(a) - f(b) = c_1(a - b) + c_2(a^2 - b^2) + ... + c_n(a^n - b^n)$$

and each term in the sum is a multiple of n by theorem 2.9. The result follows. □

Example 2.17. Let f be a polynomial with integer coefficients and let a be a positive integer such that $f(a) \neq 0$. Prove that there are infinitely many positive integers b such that $f(a) \mid f(b)$.

Proof. We take $b = a + k|f(a)|$ with k a positive integer. Then

$$f(a) \mid k|f(a)| = b - a \mid f(b) - f(a)$$

and so $f(a) \mid f(b)$. Since k is arbitrary, the result follows. □

2.1.2 Divisibility and order relation

Another key property of the divisibility relation that we want to emphasize in this section is its relationship with the usual order on the set of integers: the next proposition roughly says that a divisor of a number cannot exceed that number. One has to be a little bit careful when making such a statement (note that 1 is a divisor of -2, but it is certainly not less than -2), so we formalize this as follows:

Proposition 2.18. *If a divides b* ***and*** *$b \neq 0$, then $|a| \leq |b|$.*

Proof. Write $b = ac$, then $c \neq 0$ (since $b \neq 0$), hence $|b| = |a| \cdot |c| \geq |a|$. □

Remark 2.19. The hypothesis $b \neq 0$ is crucial in the previous proposition. The number 0 plays a very special role: it is the only integer having infinitely many divisors. More precisely, 0 is divisible by all integers, since if a is any integer, then $0 = a \cdot 0$. On the other hand, if $n \in \mathbf{Z}$ has infinitely many divisors, then necessarily $n = 0$: otherwise, by the previous proposition any divisor d of n satisfies $d \in \{-|n|, ...0, 1, ..., |n|\}$, hence n has only finitely many divisors. The next example is a nice illustration of this important observation.

Example 2.20. (Russia 1964) Let a, b be integers and let n be a positive integer such that $k - b \mid k^n - a$ for infinitely many integers k. Prove that $a = b^n$.

Proof. For any integer k we have $k - b \mid k^n - b^n$, so if $k - b \mid k^n - a$, then

$$k - b \mid (k^n - b^n) - (k^n - a) = a - b^n.$$

Using the hypothesis of the problem, we deduce that $a - b^n$ has infinitely many divisors and so $a - b^n = 0$. The result follows. □

One of the consequences of the previous proposition is the following property of the divisibility relation.

Corollary 2.21. *If a, b are integers such that $a \mid b$ and $b \mid a$, then $|a| = |b|$, i.e. $a = \pm b$.*

Proof. Everything is clear if $a = 0$ or $b = 0$. Otherwise, the previous proposition gives $|a| \leq |b|$ and $|b| \leq |a|$, thus $|a| = |b|$. □

Example 2.22. Find all integers n such that $a-b \mid a^2+b^2-nab$ for all distinct integers a, b.

Proof. The identity $a^2+b^2-nab = (a-b)^2+(2-n)ab$ shows that $a-b|(2-n)ab$ for all $a \neq b \in \mathbb{Z}$ Taking $b = 1$ and $a = k+1$, with k a positive integer, we deduce that $k \mid (2-n)(k+1) = (2-n)k+2-n$ and so $k \mid 2-n$. Hence $2-n$ has infinitely many divisors and $n = 2$. Conversely, $n = 2$ is a solution of the problem. □

Example 2.23. (Putnam 2007) Let f be a nonconstant polynomial with positive integer coefficients. Prove that if n is a positive integer, then $f(n)$ divides $f(f(n)+1)$ if and only if $n = 1$.

Proof. We have $f(f(n)+1) \equiv f(1) \pmod{f(n)}$. If $n = 1$, then this implies that $f(f(n)+1)$ is divisible by $f(n)$. Otherwise, $0 < f(1) < f(n)$ since f is nonconstant and has positive coefficients, so $f(f(n)+1)$ cannot be divisible by $f(n)$. □

Example 2.24. a) Prove that for any positive integer n there are distinct positive integers x and y such that $x+j$ divides $y+j$ for $j = 1, 2, 3, \ldots, n$.

b) Suppose that x, y are positive integers such that $x+j$ divides $y+j$ for all positive integers j. Prove that $x = y$.

Proof. a) We have $x+j \mid y+j$ if and only if $x+j \mid (y+j)-(x+j) = y-x$. Thus it is enough to ensure that $y-x$ is a multiple of $(x+1)(x+2)...(x+n)$, for instance $y = x+(x+1)(x+2)...(x+n)$.

b) Arguing as in a), we see that $y-x$ must be a multiple of $x+j$ for all positive integers j. Remark 2.19 yields $y = x$ and we are done. □

Example 2.25. Let f be a polynomial with integer coefficients, of degree $n > 1$. What is the maximal number of consecutive integers belonging to the sequence $f(1), f(2), f(3), ...$?

Proof. For the polynomial $f(X) = X + (X-1)(X-2)...(X-n)$ we have $f(1) = 1, f(2) = 2, ..., f(n) = n$, thus we have n consecutive numbers in the sequence $f(1), f(2), ...$ We will prove that we cannot have more. Assume for contradiction that we can find positive integers $a_1, ..., a_{n+1}$ and an integer x such that $f(a_i) = x + i$ for $1 \leq i \leq n+1$. Then $f(a_{i+1}) - f(a_i) = 1$ is a multiple of $a_{i+1} - a_i$, thus $a_{i+1} - a_i$ equals 1 or -1 for all i. Since $a_1, ..., a_{n+1}$ are clearly pairwise distinct (since so are their images by f), we deduce that we cannot have sign changes in the sequence $a_2 - a_1, a_3 - a_2, ..., a_{n+1} - a_n$ (indeed, otherwise there would exist i such that $a_{i+1} - a_i$ is the opposite of $a_{i+2} - a_{i+1}$, which would force $a_i = a_{i+2}$). Thus the sequence $a_2 - a_1, a_3 - a_2, ..., a_{n+1} - a_n$ must either consist only of 1's or only of -1's. We can thus find a sign ε such that $a_{i+1} - a_i = \varepsilon$ for all i. But then $a_i = a_1 + \varepsilon \cdot (i-1)$ for all i, hence $f(a_1 - \varepsilon + \varepsilon \cdot i) = x + i$ for $1 \leq i \leq n+1$. We deduce that the polynomial $f(a_1 - \varepsilon + \varepsilon \cdot X) - x - X$ has at least $n+1$ distinct roots, which is impossible since it has degree precisely n. This proves that the answer of the problem is n. □

Example 2.26. Let f be a polynomial with integer coefficients, of degree $n \geq 2$. Prove that the equation $f(f(x)) = x$ has at most n integral solutions.

Proof. Let x, y be distinct integers such that $f(f(x)) = x$ and $f(f(y)) = y$. Then $x - y = f(f(x)) - f(f(y))$ is a multiple of $f(x) - f(y)$, which in turn is a multiple of $x - y$. Thus necessarily $|f(x) - f(y)| = |x - y|$. Consider now integers $a_1 < ... < a_d$ such that $f(f(a_i)) = a_i$ for $1 \leq i \leq d$. Then the previous observation yields $|f(a_i) - f(a_j)| = a_j - a_i$ for $i < j$. We claim that the sequence $f(a_1), ..., f(a_d)$ is either increasing or decreasing. Indeed, we have

$$|f(a_{i+1}) - f(a_i) + f(a_{i+2}) - f(a_{i+1})| = |f(a_{i+2}) - f(a_i)|$$

$$= a_{i+2} - a_i = |f(a_{i+1}) - f(a_i)| + |f(a_{i+2}) - f(a_{i+1})|,$$

therefore $f(a_{i+1}) - f(a_i)$ and $f(a_{i+2}) - f(a_{i+1})$ must have the same sign for all i, proving the claim.

Assume that $f(a_1), ..., f(a_n)$ is increasing (the other case is similar). Then necessarily $f(a_{i+1}) - f(a_i) = a_{i+1} - a_i$ for all i, in other words there is some

number c such that $f(a_i) - a_i = c$ for $1 \leq i \leq d$. Since $f(X) - X - c$ has degree n, it can have at most n distinct roots and so $d \leq n$, as desired. □

Remark 2.27. A more general problem (in which $f \circ f$ is replaced with $f \circ f \circ ... \circ f$) was proposed at the IMO 2006.

Example 2.28. (Tournament of the Towns 2002) Let $a_1 < a_2 < ...$ be an infinite increasing sequence of positive integers such that a_n divides $a_1 + a_2 + ... + a_{n-1}$ for $n \geq 2002$. Prove that there is a positive integer n_0 such that

$$a_n = a_1 + ... + a_{n-1}$$

for all $n \geq n_0$.

Proof. By hypothesis, there is a sequence $x_{2002}, x_{2003}, ...$ of positive integers such that for all $n \geq 2002$ we have

$$a_1 + a_2 + ... + a_{n-1} = x_n a_n.$$

Write the previous relation with $n + 1$ instead of n and subtract the two resulting relations. We obtain

$$x_{n+1}a_{n+1} = x_n a_n + a_n = a_n(x_n + 1) \tag{1}$$

We deduce that

$$x_{n+1} = \frac{a_n}{a_{n+1}}(x_n + 1) < x_n + 1,$$

since $a_n < a_{n+1}$. Consequently, $x_{n+1} \leq x_n$ for $n \geq 2002$. Since there is no decreasing infinite sequence of positive integers, we deduce that there is $n_0 \geq 2002$ such that for all $n \geq n_0$ we have $x_{n+1} = x_n$. Let $k = x_{n_0}$, then $x_n = k$ for $n \geq n_0$ and relation (1) becomes

$$ka_{n+1} = (k + 1)a_n$$

for $n \geq n_0$. In particular,

$$a_n = k(a_{n+1} - a_n)$$

is a multiple of k for $n \geq n_0$. Writing $a_n = kb_n$, we also have $b_n = k(b_{n+1} - b_n)$ and so $k \mid b_n$ for all n, that is $k^2 \mid a_n$ for all $n \geq n_0$. An immediate induction then shows that $k^j \mid a_n$ for all $j \geq 1$ and all $n \geq n_0$. In particular, $k^j \leq a_{n_0}$ for all $j \geq 1$, which forces $k = 1$. But then

$$a_1 + ... + a_{n-1} = ka_n = a_n$$

for $n \geq n_0$ and we are done. □

A fundamental property that easily follows from the relationship between divisibility and order relation as well as basic properties of odd and even numbers is:

Theorem 2.29. *Let n be a nonzero integer. There is a unique pair of integers (a, b) with $a \geq 0$, b odd and $n = 2^a \cdot b$.*

Proof. Let us start by proving uniqueness. Suppose that $2^a b = 2^c d$ with $a, c \geq 0$ and b, d odd, and assume that $a \neq c$. Without loss of generality, we may assume that $a < c$, then $b = 2^{c-a} d$ is even, a contradiction. Thus $a = c$ and then $b = d$.

In order to prove the existence part, consider the set of powers of 2 which divide n. This set is finite, since if 2^a divides n, then $a < 2^a \leq |n|$. Thus there is a largest integer a such that $2^a \mid n$. Write $n = 2^a b$ for some integer b. If b is even, then $b = 2c$ for some integer c and then $2^{a+1} \mid n$, contradicting the maximality of a. Thus b is odd and the result is proved. □

Remark 2.30. 1) It follows easily from the previous theorem that if a, b are integers such that ab is a power of 2, i.e. $ab = 2^n$ for some $n \geq 0$ then $|a|$ and $|b|$ (but not necessarily a and b) are also powers of 2.

2) From the uniqueness part of the theorem, it follows that if $n = 2m$ is even and an odd number d divides n, then d divides m. This is our first example of a cancellation in congruences and we will use it frequently.

Yet another result that is fairly useful in practice is the following:

Theorem 2.31. *If a is an odd integer, then for all $n \geq 0$*

$$2^{n+2} \mid a^{2^n} - 1.$$