Proof. The fact that the sequence is bounded from below is an immediate consequence of Euler's theorem 4.74. In order to prove that the sequence is bounded from above we define (for $2 \le k \le n$) $u_k = \frac{\log k}{k}$ if k is a prime and $u_k = 0$ otherwise. Letting $S_1 = 0$ and $S_k = u_2 + \ldots + u_k$ for $2 \le k \le n$, we have

$$\sum_{p \le n} \frac{1}{p} = \sum_{k=2}^{n} \frac{u_k}{\ln k} = \sum_{k=2}^{n} \frac{S_k - S_{k-1}}{\ln k} = \sum_{k=2}^{n-1} S_k \left(\frac{1}{\ln k} - \frac{1}{\ln(k+1)} \right) + \frac{S_n}{\ln n}.$$

By the previous problem

$$S_k = \sum_{p \le k} \frac{\ln p}{p} < \ln k + 4$$

for $2 \le k \le n$. Therefore

$$\sum_{p \le n} \frac{1}{p} < \frac{4}{\ln 2} + \sum_{k=2}^{n-1} \left(1 - \frac{\ln k}{\ln(k+1)} \right) + \frac{\ln n + 4}{\ln n}.$$

On the other hand for each $4 \le k \le n-1$ we have (the last inequality can be proved using the function $f(x) = \ln \ln x$)

$$1 - \frac{\ln k}{\ln(k+1)} = \frac{\ln\left(1 + \frac{1}{k}\right)}{\ln(k+1)} < \frac{1}{k \ln(k+1)} < \frac{1}{k \ln k} < \ln \ln k - \ln \ln(k-1).$$

The result follows now easily by adding the previous inequalities (note that the resulting sum is telescopic). □

8.6 Congruences for composite moduli

1. (Poland 2003) A polynomial f with integer coefficients has the property that $\gcd(f(a), f(b)) = 1$ for some integers $a \neq b$. Prove that there is an infinite set of integers S such that $\gcd(f(m), f(n)) = 1$ whenever m, n are distinct elements of S.

Proof. It suffices to prove that if $a_1, ..., a_k$ are integers such that

$$\gcd(f(a_i), f(a_j)) = 1$$

for $1 \leq i \neq j \leq k$ then there is an integer a_{k+1} different from $a_1, ..., a_k$ and such that $\gcd(f(a_i), f(a_j)) = 1$ for $1 \leq i \neq j \leq k+1$. Pick a_{k+1} such that $a_{k+1} \equiv a_i \pmod{f(a_{i+1})}$ for $1 \leq i \leq k-1$ and $a_{k+1} \equiv a_k \pmod{f(a_1)}$, which is possible by the Chinese remainder theorem. Then $f(a_{k+1}) \equiv f(a_i) \pmod{f(a_{i+1})}$ for $1 \leq i < k$ and $f(a_{k+1}) \equiv f(a_k) \pmod{f(a_1)}$. Thus $\gcd(f(a_{k+1}), f(a_{i+1})) = \gcd(f(a_i), f(a_{i+1})) = 1$ for $1 \leq i < k$ and similarly $\gcd(f(a_{k+1}), f(a_1)) = 1$, as desired. □

Remark 8.26. In particular, consider two relatively prime integers a, b. Then the problem implies that in the arithmetic progression $(an+b)_{n\geq 0}$ there is an infinite set of pairwise relatively prime numbers. This is of course a direct consequence of Dirichlet's theorem on primes in arithmetic progressions, but as the problem shows one can also prove it by purely elementary means (and with an argument which generalizes to higher degrees, for which no analogue of Dirichlet's theorem is known).

2. Prove that for all positive integers k and n there exists a set S of n consecutive positive integers such that each $x \in S$ has at least k distinct prime divisors that do not divide any other element of S.

Proof. Consider a matrix $(p_{ij})_{\substack{1\leq i\leq n \\ 1\leq j\leq k}}$ with n rows and k columns and whose entries are pairwise distinct primes greater than n. Let $R_1, ..., R_n$ be the products of the entries in rows $1, 2, ..., n$ of the matrix. Then $R_1, ..., R_n$ are pairwise relatively prime, so by the Chinese remainder theorem there is a positive integer x such that $x \equiv -i \pmod{R_i}$ for $1 \leq i \leq n$. Then $x+i$ has at least k distinct prime divisors (namely the entries of the kth row of the matrix) and none of these divides $x+j$ for $j \neq i$: if p is an entry of the matrix and $p \mid x+i$ and $p \mid x+j$ then $p \mid j-i$, contradicting the fact that $p > n$. Thus $x+1, ..., x+n$ satisfy all required properties. □

3. A lattice point is called visible if its coordinates are relatively prime integers. Prove that for any positive integer k there is a lattice point whose distance from each visible lattice point is greater than k.

Proof. It suffices to prove that for each k we can find a square of side length k with sides parallel to the coordinate axes and consisting of invisible points. In other words, we want to find distinct integers x, y such that $\gcd(x+i, y+j) > 1$ for $1 \le i, j \le k$. Consider a $k \times k$ matrix whose entries $(p_{ij})_{1\le i,j \le k}$ are pairwise distinct primes, and let $R_1, ..., R_k$ (respectively $C_1, ..., C_k$) be the products of the numbers in rows (respectively columns) $1, 2, ..., k$ of the matrix. Then $R_1, ..., R_k$ (respectively $C_1, ..., C_k$) are pairwise relatively prime, so by the Chinese remainder theorem there are integers $x \neq y$ such that $x \equiv -i \pmod{R_i}$ for $1 \le i \le k$ and $y \equiv -j \pmod{C_j}$ for $1 \le j \le k$. Then for all $1 \le i, j \le k$ the prime p_{ij} divides both $x + i$ and $y + j$, hence $\gcd(x+i, y+j) > 1$ and we are done. □

4. a) Prove that for all $n \ge 1$ there is a positive integer a such that $a, 2a, ..., na$ are all perfect powers.

b) (Balkan 2000) Prove that for all $n \ge 1$ there is a set A of n positive integers such that for all $1 \le k \le n$ and all $x_1, x_2, ..., x_k \in A$ the number $\frac{x_1+x_2+...+x_k}{k}$ is a perfect power.

Proof. a) Choose pairwise distinct primes $p_1, ..., p_n$. We will prove that there is $a > 1$ such that ia is a p_ith power for $1 \le i \le n$. Letting $q_1, ..., q_k$ be all primes not exceeding n, we can write each $1 \le i \le n$ as $i = q_1^{\alpha_{i1}} ... q_k^{\alpha_{ik}}$ with $\alpha_{ij} \ge 0$. We look for a of the form $a = q_1^{x_1} ... q_k^{x_k}$. If $1 \le i \le n$, then $ia = q_1^{\alpha_{i1}+x_1} ... q_k^{\alpha_{ik}+x_k}$ is a p_ith power if $\alpha_{ij} + x_j \equiv 0 \pmod{p_i}$ for $1 \le j \le k$. By the Chinese remainder theorem we can choose for each $1 \le j \le k$ a positive integer x_j such that $x_j \equiv -\alpha_{ij} \pmod{p_i}$ for $1 \le i \le k$ and the problem is solved.

Let us remark that there is also a very simple inductive proof: we prove the result by induction on n, taking $a = 4$ for $n = 1$. Suppose that we can find a such that $ka = x_k^{y_k}$ for $1 \le k \le n$, where x_k, y_k are integers greater than 1. Let m be a common multiple of $y_1, ..., y_n$ and choose $b = (n+1)^m a^{m+1}$. For $1 \leq k \leq n$ the number kb is a y_kth power since $y_k \mid m$ and since ka is an y_kth power. On the other hand $(n+1)b = ((n+1)a)^{m+1}$ is also a perfect power, so we are done.

b) By part a) there is a positive integer a such that $a, 2a, ..., n \cdot n!a$ are all perfect powers. Consider the set $A = \{n!a, 2n!a, ..., nn!a\}$. If $x_1, ..., x_k \in A$ and $1 \leq k \leq n$, then $\frac{x_1+...+x_k}{k}$ is of the form $\frac{n!}{k}am$ with $1 \leq m \leq nk$. Thus $\frac{x_1+...+x_k}{k}$ is indeed a perfect power by the choice of a. □

5. Let a, b, c be pairwise distinct positive integers. Prove that there is an integer n such that $a+n, b+n, c+n$ are pairwise relatively prime.

Proof. It is not difficult to see that there is k such that at least two of the numbers $a+k, b+k, c+k$ are odd. Replacing a, b, c with $a+k, b+k, c+k$ and making a permutation of these numbers, we may assume that a and b are odd. Let $p_1, ..., p_m$ be the odd prime divisors of $(a-b)(b-c)(c-a)$ (we allow $m = 0$). For all $1 \leq i \leq m$ the numbers a, b, c give at most two different remainders when divided by p_i (since p_i divides $a-b$ or $b-c$ or $c-a$), thus (since $p_i > 2$) there is an integer n_i such that $a+n_i, b+n_i, c+n_i$ are not multiples of p_i. Using the Chinese remainder theorem, we can find an even integer n such that $n \equiv n_i \pmod{p_i}$ for $1 \leq i \leq m$. Then $n+a, n+b, n+c$ are pairwise relatively prime: by construction the only possible common prime factor of any two of the numbers $n+a, n+b, n+c$ is 2 (note that any such prime factor would divide $(a-b)(b-c)(c-a)$), which is excluded since $n+a$ and $n+b$ are odd. The result follows. □

6. (AMM) Prove that there are arbitrarily long sequences of consecutive integers, none of which can be written as the sum of two perfect squares.

Proof. Letting n be a positive integer, we will construct a positive integer x such that none of the numbers $x+1, ..., x+n$ is a sum of two squares. For this, we choose pairwise distinct primes $p_1, ..., p_n$ that are congruent to 3 modulo 4 (this is possible thanks to example 4.56), and then use the Chinese remainder theorem to find x such that

$$x+1 \equiv p_1 \pmod{p_1^2},\ x+2 \equiv p_2 \pmod{p_2^2}, ..., x+n \equiv p_n \pmod{p_n^2}.$$

By theorem 5.60 none of the numbers $x+1, ..., x+n$ is a sum of two squares. □

7. Let f be a nonconstant polynomial with integer coefficients and let n and k be positive integers. Prove that there is a positive integer a such that each of the numbers $f(a), f(a+1), \dots, f(a+n-1)$ has at least k distinct prime divisors.

Proof. Choose pairwise distinct prime numbers $(p_{ij})_{1\le i,j\le k}$ such that $f(x_{ij}) \equiv 0 \pmod{p_{ij}}$ for some positive integers x_{ij}, which is possible using Schur's theorem 4.67. Thanks to the Chinese remainder theorem, we can find $a \ge 1$ such that $a+i-1 \equiv x_{ij} \pmod{p_{ij}}$ for all i, j. But then each of the numbers $f(a), f(a+1), \dots, f(a+n-1)$ has at least k distinct prime divisors, since p_{ij} divides $f(a+i-1)$ for all $1 \le i, j \le k$. □

8. (IMC 2013) Let p and q be relatively prime positive integers. Prove that

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

Proof. Write

$$f(k) = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{q} \right\rfloor$$

for $0 \le k \le pq-1$. Suppose first that pq is even. If $k \in \{0, 1, ..., pq-1\}$, then writing $k = \alpha p + r$ with $0 \le r < p$ we obtain

$$\left\lfloor \frac{pq-1-k}{p} \right\rfloor = q + \left\lfloor \frac{-k-1}{p} \right\rfloor = q - \alpha - 1 = q - 1 - \left\lfloor \frac{k}{p} \right\rfloor$$

and a similar formula with p replaced by q. Since $p+q$ must be odd in this case, it follows that

$$f(pq-1-k) = q+p-2-f(k) \equiv 1+f(k) \pmod 2,$$

which immediately yields

$$\sum_{k=0}^{pq-1}(-1)^{f(k)} = \sum_{k=0}^{pq-1}(-1)^{f(pq-1-k)} = -\sum_{k=0}^{pq-1}(-1)^{f(k)}$$

and then $\sum_{k=0}^{pq-1}(-1)^{f(k)} = 0$.

Suppose now that pq is odd. Writing the Euclidean division of $k \in \{0,1,...,pq-1\}$ by p and q in the form $k = a_k p + r_k$ and $k = b_k q + R_k$, we obtain (since p and q are odd)

$$f(k) = a_k + b_k \equiv k - r_k + k - R_k \equiv r_k + R_k \pmod 2.$$

Next, for each $(r, R) \in \{0,1,...,p-1\} \times \{0,1,...,q-1\}$ the Chinese remainder theorem yields the existence of a unique $k \in \{0,1,...,pq-1\}$ such that $(r_k, R_k) = (a, b)$. We conclude that

$$\sum_{k=0}^{pq-1}(-1)^{f(k)} = \sum_{a=0}^{p-1}\sum_{b=0}^{q-1}(-1)^{a+b} = \sum_{a=0}^{p-1}(-1)^a \cdot \sum_{b=0}^{q-1}(-1)^b = 1.$$

The result follows. □

9. (IMO 1999 Shortlist) Find all positive integers n for which there is an integer m such that $2^n - 1 \mid m^2 + 9$.

Proof. Clearly $n = 1$ is a solution of the problem, so assume from now on that $n \geq 2$. If $2^n - 1 \mid m^2 + 9$ for some integer m, then $2^n - 1$ has no prime divisor $p > 3$ such that $p \equiv 3 \pmod 4$, by corollary 5.28. On the other hand, if $d > 1$ is an odd integer, then $2^d - 1 \equiv -1 \pmod 4$ and 3 does not divide $2^d - 1$, thus $2^d - 1$ has a prime factor $p \equiv 3 \pmod 4$ different from 3. We deduce that n cannot have any odd divisor $d > 1$ (as otherwise $2^d-1 \mid 2^n-1 \mid m^2+9$, contradicting the previous observations) and so n is a power of 2.

Conversely if n is a power of 2, then n is a solution of the problem. Indeed, write $n = 2^k$ and observe that

$$2^n - 1 = 3 \cdot (2^2+1)(2^4+1)...(2^{2^{k-1}}+1).$$

Choosing $m = 3a$, it is enough to find a such that

$$(2^2+1)(2^4+1)...(2^{2^{k-1}}+1) \text{ divides } a^2+1.$$

Since the Fermat numbers $2^{2^i}+1$ are pairwise relatively prime (by example 3.12), by the Chinese remainder theorem there is an integer a such that $a \equiv 2^{2^{i-1}} \pmod{2^{2^i}+1}$ for $1 \le i \le k-1$. Then $a^2+1 \equiv 0 \pmod{2^{2^i}+1}$ for $1 \le i \le k-1$ and so $(2^2+1)(2^4+1)...(2^{2^{k-1}}+1)$ divides a^2+1. The solutions of the problem are therefore all powers of 2. □

10. (Bulgaria 2003) A finite set C of positive integers is called good if for any $k \in \mathbf{Z}$ there exist $a \neq b \in C$ such that $\gcd(a+k, b+k) > 1$. Prove that if the sum of the elements of a good set C equals 2003, then there exists $c \in C$ such that the set $C - \{c\}$ is good.

Proof. Say a prime p is good for a set $C \subset \mathbf{Z}$ if for any $i \in \{0, 1, ..., p-1\}$ the congruence $x \equiv i \pmod{p}$ is satisfied by at least two elements of C. It is clear that if there is a prime p good for C, then C is good. The crucial remark is that the converse holds. Indeed, assume that C is good but no prime p is good for C. Let S be the set of all primes not exceeding $\max(C)$. Then for all $p \in S$ we can find $i_p \in \{0, 1, ..., p-1\}$ such that $x \equiv i_p \pmod{p}$ for at most one element x of C. Using the Chinese remainder theorem, we can find an integer k such that $k \equiv -i_p \pmod{p}$ for all $p \in S$. Since C is good, there are $a \neq b \in C$ such that $\gcd(a+k, b+k) > 1$. Letting p be a prime divisor of $\gcd(a+k, b+k)$, we have $p \in S$, since $p \mid b-a$ and $|a-b| < \max(C)$. But then $a \equiv -k \equiv i_p \pmod{p}$ and $b \equiv i_p \pmod{p}$, contradicting the choice of i_p. This establishes the claim.