Problemen

| Problem Section

This Problem Section is open to everyone; everybody is encouraged to send in solutions and propose problems. Group contributions are welcome. For each problem, the most elegant correct solution will be rewarded with a book token worth €20. (To compete for the book token you should have a postal address in The Netherlands.)
Please send your submission by e-mail (LaTeX is preferred), including your name and address to problems@nieuwarchief.nl.
The deadline for solutions to the problems in this edition is 1 September 2017.

Problem A

Show that there are no infinite antichains for the partial order $\leq$ on $\mathbb{N}^k$ defined by $(x_1, x_2, \ldots, x_k) \leq (y_1, y_2, \ldots, y_k)$ iff $x_i \leq y_i$ for all i, $1 \leq i \leq k$.

Problem B

A sector is a portion of a disk enclosed by two radii and an arc. For each pair of radii, there are two complementary sectors. If the two complementary sectors have unequal area, then we say that the larger sector is the major sector.
Let S be a subset of the plane. We say that $x \in S$ is virtually isolated if x is the only element of S in a major sector of a disk centered on x. Suppose that all elements of S are virtually isolated. Prove that S is countable.

Problem C (proposed by Hendrik Lenstra)

Let n be a natural number > 1. Suppose that for every prime $p < n$ we have that $p^n \equiv (p-1)^n + 1 \bmod n^2$. Prove that $n = 2$.

Edition 2016-4 We received solutions from Pieter de Groen, Alex Heinis and Toshihiro Shimizu.

Problem 2016-4/A (folklore)

For a finite sequence $s = (s_1, \ldots, s_n)$ of positive integers, denote by $p(s)$ the number of ways to write s as a sum $s = \sum_{i=1}^{n} a_i e_i + \sum_{j=1}^{n-1} b_j (e_j + e_{j+1})$ with all a_i and b_j non-negative. Here e_i denotes the sequence of which the i-th term is 1 and of which all the other terms are 0.
Show that there exists an integer $B > 1$ such that for any product F of (positive) Fibonacci numbers, there exists a finite sequence $s = (s_1, \ldots, s_n)$ with all $s_i \in \{1, 2, \ldots, B\}$ such that $p(s) = F$.

Solution We received solutions from Pieter de Groen, Alex Heinis and Toshihiro Shimizu. The book token goes to Pieter de Groen. The following solution is based on that of Alex Heinis.
Let $s = (s_1, \ldots, s_m)$ be a finite sequence of positive integers. We say that s is *left safe* if $s_1 \geq s_2$, *right safe* if $s_m \geq s_{m-1}$, and *safe* if they are both left safe and right safe. Let $s = (s_1, \cdots, s_m)$, $t = (t_1, \cdots, t_n)$ be finite sequences of integers with $m, n \geq 1$. We define the *join* $s \vee t$ of s and t as the sequence $(s_1, \cdots, s_{m-1}, s_m + t_1, t_2, \cdots, t_n)$. Note that taking the join of sequences is associative.

Redactie:

Gabriele Dalla Torre
Christophe Debry
Jinbi Jin
Marco Streng
Wouter Zomervrucht

Problemenrubriek NAW
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden

problems@nieuwarchief.nl
www.nieuwarchief.nl/problems

Moreover, if $s=(s_1,\ldots,s_m)$ is a finite sequence of positive integers, define

$$V(s)=\left\{(a,b)\in\mathbb{Z}^n_{\geq 0}\times\mathbb{Z}^{n-1}_{\geq 0}: s=\sum_{i=1}^{n}a_ie_i+\sum_{j=1}^{n-1}b_j(e_j+e_{j+1})\right\},$$

so that $\#V(s)=p(s)$, and define

$$W(s)=\left\{b\in\mathbb{Z}^{n-1}_{\geq 0}: s\geq\sum_{j=1}^{n-1}b_j(e_j+e_{j+1})\right\}$$

(where we take the usual partial order on the set of finite sequences of some fixed

$$b\mapsto\left(s-\sum_{j=1}^{n-1}b_j(e_j+e_{j+1}),b\right)$$

length). Then we have a bijection $V(s)\to W(s)$ given by $(a,b)\mapsto b$, with inverse , so also $\#W(s)=p(s)$. We will then show the following.

Lemma. *Let s be a right safe sequence, and let t be a left safe sequence. Then $p(s\vee t)=p(s)p(t)$.*

Proof. Write $s=(s_1,\ldots,s_m)$ and $t=(t_1,\ldots,t_n)$. Since for any $b\in W(s)$and $c\in W(t)$, we have $s_m+t_1\geq b_{m-1}+c_1$, concatenation of sequences defines a map $W(s)\times W(t)\to W(s\vee t)$. Since s is right safe, for any $d\in W(s\vee t)$, we have $s_m\geq s_{m-1}\geq d_{m-2}+d_{m-1}\geq d_{m-1}$, so we have a map $W(s\vee t)\to W(s)$ sending $(d_i)_{i=1}^{m+n-2}$ to $(d_i)_{i=1}^{m-1}$. By a similar argument, since t is left safe, we have a map $W(s\vee t)\to W(t)$ sending $(d_i)_{i=1}^{m+n-2}$ to $(d_{m-1+i})_{i=1}^{n-1}$, and therefore also a map $W(s\vee t)\to W(s)\times W(t)$, which by construction is the inverse of the concatenation map. Hence $p(s\vee t)=p(s)p(t)$. □

Now we return to the problem. Let F_n be the n-th Fibonacci number, where we take as convention $F_0=F_1=1$. Let $F=\prod_{i=1}^{n}F_{m_i}$ be a product of Fibonacci numbers. We may assume that each F_{m_i} is at least 2, that F_2 occurs at most twice (since $F_5=8$), and therefore that if $m_i=2$, then $i=1$ or $i=n$.
Let s_i denote the sequence of m_i ones; it is well-known then that $p(s_i)=F_{m_i}$ for all i. Then note that s_1 is right safe, that all s_i with $2\leq i\leq n-1$ are of length at least 3 and safe, and that s_n is left safe. Moreover, as s_i has length 3 if $2\leq i\leq n-1$, we see that $s_1\vee\cdots\vee s_i$ is right safe if $2\leq i\leq n-1$. Hence inductively applying the lemma gives $p(s_1\vee\cdots\vee s_n)=\prod_{i=1}^{n}p(s_i)=F$, as required.

Problem 2016-4/B (folklore)

Let ℓ be a prime number. For any group homomorphism $f:A\to B$ between abelian groups and for any integer $n\geq 0$, denote by f_n the induced homomorphism $A/\ell^nA\to B/\ell^nB$. Let $(k_n)_{n=0}^{\infty}$ and $(c_n)_{n=0}^{\infty}$ be sequences of integers.
Show that there exist integers $N,a,b\geq 0$ and a group homomorphism $f:(\mathbb{Z}/\ell^N\mathbb{Z})^a\to(\mathbb{Z}/\ell^N\mathbb{Z})^b$ such that for all $n\geq 0$ we have $\#\ker f_n=\ell^{k_n}$ and $\#\operatorname{coker} f_n=\ell^{c_n}$ if and only if $k_0=c_0=0$ and the sequences $(k_{n+1}-k_n)_{n=0}^{\infty}$ and $(c_{n+1}-c_n)_{n=0}^{\infty}$ are non-negative, non-increasing, eventually zero, and there is a constant C such that for all n such that $k_{n+1}-k_n$ and $c_{n+1}-c_n$ are not both zero, their difference is C.
(Recall that the *cokernel* $\operatorname{coker} f$ of a group homomorphism $f:A\to B$ between abelian groups is the quotient of B by the image of f.)

Solution We received a solution from Alex Heinis, who is also rewarded the book token for this problem. The second part of the following solution is similar to that of Alex Heinis.
Write $A=(\mathbb{Z}/\ell^N\mathbb{Z})^a$ and $B=(\mathbb{Z}/\ell^N\mathbb{Z})^b$, and write $A_n=A/\ell^nA$ and $B_n=B/\ell^nB$. Moreover, for all $n\geq 0$, let $k_n=\frac{\log(\#\ker f_n)}{\log\ell}$. We show they satisfy the required properties.
For all $n\geq 0$, let $i_n=\frac{\log(\#\operatorname{im} f_n)}{\log\ell}$. Note that the quotient map $B\to B_n$ sends $\operatorname{im} f$ to $\operatorname{im} f_n$, and the induced map $\operatorname{im} f\to\operatorname{im} f_n$ is surjective with kernel $\operatorname{im} f\cap\ell^nB$. By the structure theorem for finitely generated abelian groups (and as $\operatorname{im} f$ is ℓ^N-torsion), there exist unique $t_1,\ldots,t_N\geq 0$ such that $\operatorname{im} f\cong\bigoplus_{i=1}^{N}(\mathbb{Z}/\ell^i\mathbb{Z})^{t_i}$. Moreover, we have $\ell^nB=B[\ell^{N-n}]$ if $n\leq N$ and $\ell^nB=0$ otherwise, so $\operatorname{im} f\cap\ell^nB=(\operatorname{im} f)[\ell^{N-n}]$ if $n\leq N$ and $\operatorname{im} f\cap\ell^nB=0$ otherwise.

We deduce that

$$i_n = \sum_{j=1}^{N} jt_j - \sum_{j=1} \min(j, N-n)\, t_j$$
$$= \sum_{j=1}^{N} \max(j+n-N, 0)\, t_j = \sum_{j=N-n+1} (j+n-N)\, t_j,$$

and that $i_n = \sum_{j=1}^{N} jt_j$ otherwise.
Therefore, for all $n \geq N$ we have $i_{n+1} - i_n = 0$. Moreover, note that $i_{n+1} - i_n = \sum_{j=N-n}^{N} t_j$ if $n < N$, so that $(i_{n+1} - i_n) - (i_n - i_{n-1}) = t_{N-n}$ for all $1 \leq n < N$.
First note that $k_0 = c_0 = 0$, and $k_n, c_n \geq 0$ for all $n \geq 0$ (as ℓ to that power is the order of a group). Now we use the isomorphisms $A_n / \ker f_n \to \operatorname{im} f_n$ and $B_n / \operatorname{im} f_n \to \operatorname{coker} f_n$ to see that we have $k_n = \min(n,N)\, a - i_n$ and $c_n = \min(n,N)\, b - i_n$ for all n. Therefore:

– If $1 \leq n < N$, then

$$(k_{n+1} - k_n) - (k_n - k_{n-1}) = (c_{n+1} - c_n) - (c_n - c_{n-1})$$
$$= (i_n - i_{n-1}) - (i_{n+1} - i_n) = -t_{N-n} \leq 0$$

– If $n \geq N$, then $k_{n+1} - k_n = c_{n+1} - c_n = 0$;
– Moreover, $k_N - k_{N-1} = a - i_N + i_{N-1} = a - \sum_{j=1}^{N} t_j$, and $c_N - c_{N-1} = b - \sum_{j=1}^{N} t_j$

As $\sum_{j=1}^{N} t_j$ is the minimum number of generators of $\operatorname{im} f$ and A maps surjectively to $\operatorname{im} f$, it follows that $k_N - k_{N-1} \geq 0$. As $\sum_{j=1}^{N} t_j$ is the dimension over $\mathbb{F}_\ell$ of $(\operatorname{im} f)[\ell]$ and $(\operatorname{im} f)[\ell] \subseteq B[\ell]$, it follows that $c_N - c_{N-1} \geq 0$. Therefore we see that $(k_{n+1} - k_n)_{n=0}^{\infty}$ and $(c_{n+1} - c_n)_{n=0}^{\infty}$ are non-increasing sequences that are eventually zero, hence they are non-negative as well.
Finally, note that for $n < N$, we have $(k_{n+1} - k_n) - (c_{n+1} - c_n) = a - b$, which shows that the sequences $(k_n)_{n=0}^{\infty}$ and $(c_n)_{n=0}^{\infty}$ satisfy the required conditions.
For the converse, suppose that $(k_n)_{n=0}^{\infty}$ and $(c_n)_{n=0}^{\infty}$ satisfy the conditions in the problem. Let N be the smallest integer $n \geq 0$ for which $k_{n+1} - k_n = c_{n+1} - c_n = 0$. Let for $0 \leq n < N$, $r_n = (k_n - k_{n-1}) - (k_{n+1} - k_n) = (c_n - c_{n-1}) - (c_{n+1} - c_n)$, which is non-negative as the sequences $(k_{n+1} - k_n)_{n=0}^{\infty}$ and $(c_{n+1} - c_n)_{n=0}^{\infty}$ are non-increasing. Moreover, let $s_k = k_N - k_{N-1}$ and let $s_c = c_N - c_{N-1}$. Consider the map

$$f : (\mathbb{Z}/\ell^N\mathbb{Z})^{s_k} \oplus \bigoplus_{n=1}^{N-1} (\mathbb{Z}/\ell^N\mathbb{Z})^{r_n} \to (\mathbb{Z}/\ell^N\mathbb{Z})^{s_c} \oplus \bigoplus_{n=1}^{N-1} (\mathbb{Z}/\ell^N\mathbb{Z})^{r_n}$$

of which the matrix in block form (with respect to the given splitting into summands) is the diagonal matrix with diagonal $(0_{s_c \times s_k}, \ell \cdot I_{r_1}, \ell^2 \cdot I_{r_2}, \ldots, \ell^{N-1} \cdot I_{r_{N-1}})$.
A couple of observations: first note that if $n \geq N$, then $f_n = f$. Moreover, we note that for $n < N$, the induced map

$$f_n : (\mathbb{Z}/\ell^n\mathbb{Z})^{s_k} \oplus \bigoplus_{i=1}^{N-1} (\mathbb{Z}/\ell^n\mathbb{Z})^{r_i} \to (\mathbb{Z}/\ell^n\mathbb{Z})^{s_c} \oplus \bigoplus_{i=1}^{N-1} (\mathbb{Z}/\ell^n\mathbb{Z})^{r_i}$$

is given by the same matrix as the one defining f. And finally, we note that therefore $\ker f_n = \ker 0_{s_c \times s_k} \oplus \bigoplus_{i=1}^{N-1} \ker(\ell^i \cdot I_{r_i})$.
Let us show by induction on n that $\#\ker f_n = \ell^{k_n}$ and $\#\operatorname{coker} f_n = \ell^{c_n}$ for all n. First of all, for $n = 0$, note that f_0 is the map $0 \to 0$, so $k_0 = c_0 = 0$. Now let $0 < n \leq N$, and suppose that $\#\ker f_{n-1} = \ell^{k_{n-1}}$ and $\#\operatorname{coker} f_{n-1} = \ell^{c_{n-1}}$. Note that $\#\ker f_n = \ell^{n s_k + \sum_{i=1}^{N-1} \min(i,n) r_i}$ and that $\#\ker f_{n-1} = \ell^{(n-1)s_k + \sum_{i=1}^{N-1} \min(i,n-1) r_i}$. Therefore $\#\ker f_n / \#\ker f_{n-1} = \ell^{s_k + \sum_{i=n}^{N-1} r_i}$; by definition of s_k and the r_i, the exponent is by a telescoping sum equal to $k_n - k_{n-1}$. Hence $\#\ker f_n = \ell^{k_n - k_{n-1}} \#\ker f_{n-1} = \ell^{k_n}$. Similarly, we show that $\#\operatorname{coker} f_n = \ell^{c_n}$.
Finally, we note that for $n > N$, we have $\#\ker f_n = \#\ker f_N = \ell^{k_N} = \ell^{k_n}$, as for all $i > N$, we have $k_{i+1} - k_i = 0$; and similarly, we have $\#\operatorname{coker} f_n = \ell^{c_n}$.

Problem 2016-4/C (folklore)

Let R be the polynomial ring over $\mathbb{Z}$ with variables x_i, y_i, z_i for all $i \in \mathbb{Z}$. Let S be the polynomial ring over $\mathbb{Z}$ with variables t_i for all $i \in \mathbb{Z}$. Let $\tau : R \to R$ be the isomorphism of rings given by $x_i \mapsto x_{i+1}$, $y_i \mapsto y_{i+1}$ and $z_i \mapsto z_{i+1}$.

Consider the morphism $f: R \to S$ of rings given by $x_i \mapsto t_{i-1}t_it_{i+1}$, $y_i \mapsto t_i^3$ and $z_i \mapsto t_i^2$. Does there exist a finite number of elements $r_1, \ldots, r_n \in R$ such that the kernel I of f is generated as an ideal in R by $\{\tau^i r_j: i \in \mathbb{Z}, j = 1, \ldots, n\}$?

Solution We received no solutions for this problem. The answer is no.
We assume monomials to be monic. Moreover, we will abuse notation by setting $\tau : S \to S$ to be the automorphism of rings sending t_i to t_{i+1} for all $i \in \mathbb{Z}$. Let $M \subseteq R$ denote the set of monomials of R, and let $N \subseteq S$ denote the set of monomials of S. Then f maps M into N. Moreover, identifying (as groups) R with $\bigoplus_{m\in M} \mathbb{Z} \cdot m$ and S with $\bigoplus_{n \in N} \mathbb{Z} \cdot n$, we see that $f: R \to S$ is given by

$$\sum_{m \in M} x_m m \mapsto \sum_{n \in N} \left(\sum_{m \in f^{-1}(n)} x_m \right) n,$$

for x_m zero for all but finitely many $m \in M$. Finally, we note that for all $x \in R$, we have $f(\tau x) = \tau f(x)$.
Let, for $x = \sum_{m \in M} x_m m \in R$ and $n \in N$, the *n-th homogeneous part* be $x_n = \sum_{m \in f^{-1}(n)} x_m m$. Then note that $x \in I$, if and only if for all $n \in N$, we have $x_n \in I$, and $x = \sum_{n \in N} x_n$, where we note that x_n is zero for all but finitely many $n \in N$, as the same is true for the x_m for $m \in M$. So let us say that an element of the form $\sum_{m \in f^{-1}(n)} x_m m$ in R is *homogeneous with respect to n*.
Write $R_n = \bigoplus_{m \in f^{-1}(n)} \mathbb{Z} \cdot m$. Then note that $f|_{R_n}$ is injective if and only if $\# f^{-1}(n) \leq 1$. So consider the set $N' \subseteq N$ of $n \in N$ such that $\# f^{-1}(n) \geq 2$, where we take the partial order on N given by divisibility by an element of $f(M)$, i.e. $n \leq n'$ if there exists an $m \in M$ such that $nf(m) = n'$.
Define, for integers $k \geq 1$ and i, the monomial $n_{k,i} = t_i^3 t_{i+1} t_{i+2} \cdots t_{i+3k-1} t_{i+3k}^3$. We determine $f^{-1}(n_{k,i})$. Let $m \in f^{-1}(n_{k,i})$. Since n only has two exponents of at least 2, we see that the total y,z-degree of m is at most 2. Moreover, the degree of n is $3k+5$, so comparing degrees modulo 3, we see that m must be divisible by either $y_i z_{i+3k}$ or $y_{i+3k} z_i$. In the first case, write $m = m' y_i z_{i+3k}$, and note that $f(m') = t_{i+1} \cdots t_{i+3k}$. By induction on k, one can show that m' must be equal to $x_{i+2} x_{i+5} \cdots x_{i+3k-1}$, therefore m must be $m_{k,i,1} = x_{i+2} x_{i+5} \cdots x_{i+3k-1} y_i z_{i+3k}$. In the same way, one shows in the second case that m must be equal to $m_{k,i,2} = x_{i+1} x_{i+4} \cdots x_{i+3k-2} y_{i+3k} z_i$. Since both of them do map to $n_{k,i}$, we find that $f^{-1}(n_{k,i}) = \{m_{k,i,1}, m_{k,i,2}\}$. In particular, $n_{k,i} \in N'$, and $\ker f|_{R_{n_{k,i}}}$ is generated by $m_{k,i,1} - m_{k,i,2}$.
Moreover, $n_{k,i}$ is minimal in N'; if $n \in N'$ divides $n_{k,i}$ in $f(M)$, then for $m_1, m_2, m' \in M$ such that $m_1 \neq m_2$, $f(m_1) = f(m_2) = n$ and $f(m_1)f(m') = f(m_2)f(m') = n_{k,i}$, we have $\{m_1 m', m_2 m'\} = \{m_{k,i,1}, m_{k,i,2}\}$. Since $\gcd(m_{k,i,1}, m_{k,i,2}) = 1$, it follows that $m' = 1$ and therefore that $n = n_{k,i}$.
Now we can prove our answer. Let G be any subset of $R - \{0\}$ such that I is generated by $\{\tau^a g: a \in \mathbb{Z}, g \in G\}$. We show that G is infinite. Let G' denote the set of non-zero homogeneous parts of elements of G, and note that G is finite if and only if G' is. Then I is also generated by $\{\tau^a g': a \in \mathbb{Z}, g' \in G'\}$.
Note that for all $k \geq 1$, we have $m_{k,0,1} - m_{k,0,2} \in I$, and write $m_{k,0,1} - m_{k,0,2} = \sum_{a,g'} \alpha_{a,g'} \tau^a g'$, for some $\alpha_{a,b} \in R$ that are zero for all but finitely many pairs (a,b); we may assume that the $\alpha_{a,b}$ are homogeneous, by taking the $n_{k,0}$-th homogeneous part of this identity if necessary. If (a,g') is such that $\alpha_{a,g'} \neq 0$, and if g' is homogeneous with respect to n, then $\tau^a n \in N'$ and $\tau^a n \leq n_{k,0}$, so by minimality of $n_{k,0}$ it follows that $\tau^a n = n_{k,0}$. Moreover, $\ker f|_{R_{n_{k,0}}}$ is generated by $m_{k,0,1} - m_{k,0,2}$, so $\tau^a g'$ is a non-zero integer multiple of $m_{k,i,1} - m_{k,i,2}$. It follows that for any $k \geq 1$ there exists $g'_k \in G'$ such that g'_k is a non-zero integer multiple of $\tau^a(m_{k,0,1} - m_{k,0,2})$ for some $a \in \mathbb{Z}$. Now τ preserves total degrees, so the total degree of g'_k is that of $m_{k,0,1}$ and $m_{k,0,2}$, which is $k+2$. In particular, G' contains elements of every total degree that is at least 3, so G' (and therefore G) is infinite, as desired.

Rectification
In the list of solvers of 2016-3/B, Rob van der Waall was missing, but should have been there. We apologise for this omission.