Edition 2017-3 We received solutions from Mohammad Aassila (Strasbourg), Herbert Beltman (Amsterdam), Aart Blokhuis (Eindhoven), Bas Edixhoven (Leiden), Alex Heinis (Amsterdam), Ammar Yasir Kiliç (Hellevoetsluis), Alexander Lemmens (Leuven), Quinten Lootens (Waregem), Hans van Luipen (Zaltbommel), Hendrik Reuvers (Maastricht), Hans Samuels Brusse (Den Haag), Toshihiro Shimizu (Kawasaki) and Djurre Tijsma (Zeist). The book tokens for problems A, B and C go to Herbert Beltman, Quinten Lootens, respectively René Pannekoek.

Problem 2017-3/A

Let n be a natural number and suppose that $A_1,\dots,A_n$ are different subsets of $\{1,\dots,n\}$. Prove that there is a $k\in\{1,\dots,n\}$ such that $A_1\setminus\{k\},\dots,A_n\setminus\{k\}$ are different.

Solution Solved by Herbert Beltman, Aart Blokhuis, Ammar Yasir Kiliç, Alexander Lemmens, Hans van Luipen, Hendrik Reuvers, Hans Samuels Brusse, Toshihiro Shimizu en Djurre Tijsma. The solutions are all very similar. Below is Toshihiro Shimizu's solution. The book token has to stay at home and goes to Herbert Beltman.

By contradiction. We assume that for any integer $k=1,2,\dots,n$, we can select $i\neq j$ such that $A_i\setminus\{k\}=A_j\setminus\{k\}$ i.e. $A_i=A_j\sqcup\{k\}$ or $A_j=A_i\sqcup\{k\}$ where $A\sqcup B$ means $A\cup B$ and A and B are disjoint. Construct undirected graph $G=(V,E)$ with $V=\{A_1,A_2,\dots,A_n\}$. Draw an edge between A_i, A_j with label k if $A_i=A_j\sqcup\{k\}$ or $A_j=A_i\sqcup\{k\}$ (if there are multiple pairs i,j, select only one edge). Then, G has n edges. A forest graph has at most $n-1$ edges, so the graph has a cycle. Say the cycle has edges labeled $k_1,k_2,\dots,k_m$. Then, from some set A, we can get $A\sqcup\{k_1\}$ by adding or removing $k_2,k_3,\dots,k_m$. This is impossible.

Problem 2017-3/B (proposed by Hans Zantema)

Let $f,g:\mathbb{N}\to\mathbb{N}$ be strictly increasing functions. Prove that there exists an $n\in\mathbb{N}$ such that $f(g(g(n)))\geq g(f(n))$.

Solution Solved by Herbert Beltman, Aart Blokhuis, Alex Heinis, Ammar Yasir Kiliç, Alexander Lemmens, Quinten Lootens, Hans van Luipen, Hendrik Reuvers, Hans Samuels Brusse, Toshihiro Shimizu and Djurre Tijsma. All solutions are similar. Here is the solution by Quinten Lootens.

By contradiction, assume $f(g(g(n)))<g(f(n))$ for all n. Since f is strictly increasing we can say that $n\leq f(n)$. Our assumption $f(g(g(n)))<g(f(n))$ and $n\leq f(n)$ imply that $g(g(n))<g(f(n))$. Since g is increasing we have that $g(n)<f(n)$. Let us look at $g^3(n)<f(g(g(n)))<g(f(n))$, so $g^2(n)<f(n)$. Repeating this for $g^4(n)<f(g(g(n)))<g(f(n))$, we find $g^3(n)<f(n)$, et cetera. If we keep going we can prove that $g^t(n)<f(n)$ for all t. This is clearly impossible so the contradiction has been reached.

Problem 2017-3/C (proposed by René Pannekoek)

Determine all $n\in\mathbb{N}$ such that 2^n-1 divides 3^n-1.

Solution We received solutions from Mohammad Aassila, Aart Blokhuis, Bas Edixhoven, Ammar Yasir Kiliç, Alexander Lemmens and Toshihiro Shimizu. Several people wrote that they really liked this problem. That is why this time the book token goes to the contributor of the problem. René Pannekoek has also posted a similar problem online:

https://math.stackexchange.com/questions/2337536/for-which-n-does-2n1-divide-10n1

There you can also read what made him come up with this problem. All solutions involve quadratic reciprocity. Some solutions are very short and similar to the following solution by Aart Blokhuis.

For $n=1$, and depending on your definition of $\mathbb{N}$ and divisibility, $n=0$ the divisibility holds trivially, we show that these are the only n. If $n>0$ is even, then 2^n-1 is divisible by 3, and 3^n-1 clearly not, so assume $n>1$ is odd and $2^n-1\mid 3^n-1$. Let p be a prime

Redacteur: Rob Eggermont
problems@nieuwarchief.nl
www.nieuwarchief.nl/problems

factor of 2^n-1, then $3^n=1 \bmod p$, and n is odd, so the order of $3 \bmod p$ is odd, and hence 3 is a quadratic residue $\bmod p$ (because $3^{(p-1)/2}=1$). Using quadratic reciprocity we see that this means that $p=\pm 1 \bmod 12$. It follows that 2^n-1, being the product of primes that are $\pm 1 \bmod 12$ is itself $\pm 1 \bmod 12$, but if n is odd, and at least 3, then 2^n-1 is $7 \bmod 12$. Contradiction.

The following proof by Bas Edixhoven takes a different route and puts the problem in perspective. Assume that $n>1$ and n is odd. Let $N \coloneqq 2^n-1$. Then $N=1$ in $\mathbb{Z}/3\mathbb{Z}$, hence N is not divisible by 3. Hence 3 is an invertible element of the ring $\mathbb{Z}/N\mathbb{Z}$. We will show that the order of 3 in the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^\times$ is even, thereby showing that $3^n \neq 1$ in $(\mathbb{Z}/N\mathbb{Z})^\times$ (because n is odd), hence that N does not divide 3^n-1. If N is a prime number (such primes are called Mersenne primes, there are at this moment (2017) about 49 examples, see https://en.wikipedia.org/wiki/Mersenneprime), then the reader can check that quadratic reciprocity implies that 3 is not a square in $\mathbb{Z}/N\mathbb{Z}$, and hence its order in $(\mathbb{Z}/N\mathbb{Z})^\times$ is even. The proof of quadratic reciprocity via the field $\mathbb{Q}(\zeta_N)$ then motivates what follows (without the assumption that N is prime).

To show that the order of 3 in the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^\times$ is even, it suffices to give a group morphism $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{Z}/2\mathbb{Z}$ such that 3 is mapped to 1. We get such a morphism via an action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on the ring $\mathbb{Z}[\zeta_N]$ (the subring of $\mathbb{C}$ generated by $\zeta_N \coloneqq e^{2\pi i/N}$). Indeed, already Gauss showed that the polynomial $\Phi_N \coloneqq \prod_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}(X-\zeta_N^a)$ has coefficients in $\mathbb{Z}$ and is irreducible over $\mathbb{Z}$, hence $\mathbb{Z}[\zeta_N]=\mathbb{Z}[X]/(\Phi_N)$. Therefore, for each $a\in(\mathbb{Z}/N\mathbb{Z})^\times$ there is an automorphism σ_a of $\mathbb{Z}[\zeta_N]$ such that $\sigma_a(\zeta_N)=\zeta_N^a$, and the map $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}[\zeta_N])$, $a\mapsto\sigma_a$ is an morphism of groups (it is an isomorphism but we do not use that). We claim that the quadratic ring $\mathbb{Z}[\sqrt{-N}]$ is a subring of $\mathbb{Z}[\zeta_N]$, and we will prove it below; for now, assume that this is so. The composition

$$(\mathbb{Z}/N\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}[\zeta_N]) \to \mathrm{Aut}(\mathbb{Z}[\sqrt{-N}])$$

(with the second map sending σ to its restriction on $\mathbb{Z}[\sqrt{-N}]$) is then the desired morphism. Let us indeed check that 3 in $(\mathbb{Z}/N\mathbb{Z})^\times$ is sent to the non-trivial element of $\mathrm{Aut}(\mathbb{Z}[\sqrt{-N}])$. For that, we consider the automorphism σ_3 on $\mathbb{Z}[\zeta_N]/3\mathbb{Z}[\zeta_N]=\mathbb{F}_3[X]/(\Phi_N)$. Let Frob_3 denote the map $z\mapsto z^3$ from $\mathbb{F}_3[X]/(\Phi_N)$ to itself. This is a ring morphism, the 3-Frobenius map. Let $\bar{\zeta}_N$ denote the image of ζ_N in $\mathbb{Z}[\zeta_N]/3\mathbb{Z}[\zeta_N]$. As $\sigma_3(\bar{\zeta}_N)=\bar{\zeta}_N^3=\mathrm{Frob}_3(\bar{\zeta}_N)$, σ_3 induces the map Frob_3 on $\mathbb{Z}[\zeta_N]/3\mathbb{Z}[\zeta_N]$. The inclusion $\mathbb{Z}[\sqrt{-N}]\subset\mathbb{Z}[\zeta_N]$ induces a morphism of rings $\mathbb{Z}[\sqrt{-N}]/3\mathbb{Z}[\sqrt{-N}]\to\mathbb{Z}[\zeta_N]/3\mathbb{Z}[\zeta_N]$. We note that $\mathbb{Z}[\sqrt{-N}]/3\mathbb{Z}[\sqrt{-N}]=\mathbb{F}_3[X]/(X^2+N)$ and that $X^2+N=X^2+1$ in $\mathbb{F}_3[X]$ is irreducible. Therefore $\mathbb{Z}[\sqrt{-N}]/3\mathbb{Z}[\sqrt{-N}]$ is a field and the morphism of rings

$$\mathbb{Z}[\sqrt{-N}]/3\mathbb{Z}[\sqrt{-N}] \to \mathbb{Z}[\zeta_N]/3\mathbb{Z}[\zeta_N]$$

is injective, and therefore the restriction of σ_3 to $\mathbb{Z}[\sqrt{-N}]$ induces the 3-Frobenius endomorphism on $\mathbb{Z}[\sqrt{-N}]/3\mathbb{Z}[\sqrt{-N}]$, which is non-trivial.

It remains to prove the claim that $\mathbb{Z}[\sqrt{-N}]$ is a subring of $\mathbb{Z}[\zeta_N]$. We write $N=N_1N_2^2$, with N_1 square free. For every odd prime p we let $p^*\coloneqq p$ if $p=1$ in $\mathbb{Z}/4\mathbb{Z}$ and $p^*\coloneqq -p$ if $p=-1$ in $\mathbb{Z}/4\mathbb{Z}$. Gauss already showed that for every odd prime p, there is an element $g_p\in\mathbb{Z}[\zeta_p]$ such that $g_p^2=p^*$ (g_p is called a Gauss sum, and the formula is $g_p=\sum_a\varepsilon_p(a)\zeta_p^a$, where a ranges over $\mathbb{F}_p^\times$ and ε_p is the Legendre symbol). As $N_1=-1$ in $\mathbb{Z}/4\mathbb{Z}$, the number of primes p dividing N_1 with $p=-1$ in $\mathbb{Z}/4\mathbb{Z}$ is odd. Hence $-N_1=\prod_{p\mid N_1}p^*=\prod_{p\mid N_1}g_p^2$, and therefore $-N_1$ is a square in $\mathbb{Z}[\zeta_N]$, and therefore $-N$ as well.

Let us end with a few remarks. For initiated readers the proof is very natural and can be shortened much: the quadratic characters of $(\mathbb{Z}/N\mathbb{Z})^\times$ correspond to the quadratic subfields of $\mathbb{Q}(\zeta_N)$; the discriminant of $\mathbb{Q}(\sqrt{-N})$ is $-N_1$ and therefore (explicit class field theory for $\mathbb{Q}$, or call it Kronecker–Weber) $\mathbb{Q}(\sqrt{-N})$ is contained in $\mathbb{Q}(\zeta_{N_1})$. We made an effort to make the proof as short and self-contained as possible. We could have included a proof of $g_p^2=p^*$ as well, but we also liked to include two references to Gauss. There is a way around the Gauss sum argument, if one uses from Galois theory that, for every odd prime p, $\mathbb{Q}(\zeta_p)$ has a unique quadratic subfield, whose discriminant is divisible only by p and therefore equal to $\mathbb{Q}(\sqrt{p^*})$.

I would like to finish by thanking René Pannekoek for the pleasure that thinking about his problem has given me.