Problemen

Problem Section

Edition 2015-2 We received solutions from Raymond van Bommel, Alex Heinis, Jos van Kan, Thijmen Krebs, Julian Lyczak, Tejaswi Navilarekallu, Traian Viteam and Robert van der Waall.

Problem 2015-2/A (proposed by Gabriele Dalla Torre)
Show that there are infinitely many primes that divide at least one integer of the form

$$2^{n^3+1} - 3^{n^2+1} + 5^{n+1}.$$

Solution We received solutions from Raymond van Bommel, Alex Heinis, Jos van Kan, Thijmen Krebs, Tejaswi Navilarekallu, Traian Viteam and Robert van der Waall. The following is based on that of Tejaswi Navilarekallu, who also receives the book token.
Suppose for a contradiction that there are only finitely many primes that divide at least one integer of the form $f(n) = 2^{n^3+1} - 3^{n^2+1} + 5^{n+1}$. Let $P = \{p_1, p_2, \ldots, p_s\}$ be the odd primes amongst them, and let $n = 4(p_1 - 1)(p_2 - 1)\cdots(p_s - 1)$. Then $f(n) \equiv 2 - 3 + 5 \equiv 4 \not\equiv 0 \mod p$ for all $p \in P$, and $f(n) \equiv 0 - 3 + 5 \equiv 2 \mod 8$ (using that n is even and that odd squares are 1 modulo 8). Moreover, as $n > 1$, we have $f(n) = 2^{n^3+1} - 3^{n^2+1} + 5^{n+1} > 2^{(n^2+1)(n-1)} - 3^{n^2+1} + 5^{n+1} > 5^{n+1} > 8$. So by assumption, 2 is the only prime dividing $f(n)$; i.e. $f(n)$ is a power of 2 that is greater than 8 and that is 2 modulo 8, this is a contradiction.

Problem 2015-2/B (proposed by Jinbi Jin)
Let n be a positive integer. Two players, Ann and Bill, play the following game. First, Ann distributes a number of balls over boxes numbered from 1 up to n. Then Bill chooses one of the boxes, and adds a ball to it. Finally, Ann attempts to empty all boxes, using only the following moves.
- Taking one ball from three consecutive boxes.
- Taking three balls from one box.

Ann wins if she succeeds in doing so, otherwise Bill wins.
1. Determine (as a function in n) the maximum number of losing moves Bill can have. What is the minimum number of balls Ann needs to attain this number?
2. Do the same as in point 1, if Ann in addition is allowed *only once* to remove two balls from one box.

Solution We received solutions from Raymond van Bommel and Julian Lyczak, Alex Heinis and Thijmen Krebs. The following solution is loosely based on that of Raymond van Bommel and Julian Lyczak, who also receive the book token.
We will view a distribution of balls over n boxes as a map from $\{1, 2, \ldots, n\}$ to $\mathbb{Z}_{\geq 0}$; and will often write them as words of length n with alphabet $\mathbb{Z}_{\geq 0}$. We denote the distribution with a single ball in box m by $[m]$ (so that Bill adding a ball in box m to some distribution corresponds to adding $[m]$ to the distribution).
Given a distribution D of balls over n boxes, we denote by
- $\#D = \sum_{i=1}^{n} D(i)$, the number of balls in D;
- $\#_{<d}D = \sum_{i=1}^{d-1} D(i)$, the number of balls in D "to the left of" box d;
- $\#_{>d}D = \sum_{i=d+1}^{n} D(i)$, the number of balls in D "to the right of" box d;
- $a_s(D) = \sum_{i \equiv s \mod 3} D(i)$, the number of balls in D in boxes that are congruent to s modulo 3.

Moreover, let
- A_d for $1 \leq d \leq n-2$ denote the distribution $0^{d-1}1^3 0^{n-d-2}$ (a *move of type A*);
- B_d for $1 \leq d \leq n$ denote the distribution $0^{d-1}30^{n-d}$ (a *move of type B*);
- C_d for $1 \leq d \leq n$ denote the distribution $0^{d-1}20^{n-d}$ (a *move of type C*);

these correspond to the three moves Ann can perform.

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

Oplossingen

Solutions

Ad 1. Let D be a distribution of balls over n boxes. Here a losing move m for Bill is one such that $D + [m]$ can be written as the sum of moves of types A and B.
We show that the maximum number of losing moves Bill can have is $\lceil \frac{n}{3} \rceil$, and that the minimum number of balls Ann needs to achieve this is 2 balls if $n \leq 3$, and $3\lceil \frac{n}{3} \rceil - 4$ balls otherwise.
We first give examples that attain these bounds. If $n \leq 3$, then $D = 20^{n-1}$ works, as Bill has one losing move $[1]$ ($D + [1] = B_1$), and Ann uses 2 balls. If $n > 3$, then writing $\alpha = 3\lceil \frac{n}{3} \rceil - 4$, we see that $D = 01^{\alpha}0^{n-\alpha-1}$ works, as for all $i \equiv 1 \mod 3$, we have

$$D + [i] = 01^{i-1}0^{n-i} + 0^{i-1}1^{\alpha-i+2}0^{n-\alpha-1}.$$

As $\alpha \equiv -1 \mod 3$, both terms on the right can be written as a sum of moves of type A, so this shows that Bill has $\lceil \frac{n}{3} \rceil$ losing moves.
We show that $\lceil \frac{n}{3} \rceil$ is the maximum number of losing moves Bill can have. Let D be any distribution of balls over n boxes. Then note that $a_s(A_d) - a_t(A_d)$ and $a_s(B_d) - a_t(B_d)$ are both divisible by 3 for all s, t. Hence if putting a ball in box m is a losing move for Bill, then $a_s(D) - a_m(D) - 1 = a_s(D + [m]) - a_m(D + [m]) \equiv 0 \mod 3$ for all $s \not\equiv d \mod 3$. So putting a ball in any box i with $i \not\equiv m \mod 3$ is a winning move for Bill, as $a_i(D + [i]) - a_m(D + [i]) = a_i(D) + 1 - a_m(D) \equiv 2 \mod 3$, so D cannot be written as the sum of moves of types A and B. Therefore Bill can have at most $\lceil \frac{n}{3} \rceil$ losing moves, all of which must have the same value modulo 3.
Next, we show that 2 is the minimum number of balls Ann needs if $n \leq 3$, and that $3\lceil \frac{n}{3} \rceil - 4$ is the minimum number of balls she needs otherwise. Let D be any distribution of balls over n boxes. Note that $\#A_d = 3$ and $\#B_d = 3$, so for D to have losing moves, one needs $\#(D + [m]) \equiv 0 \mod 3$ for some box m. Hence $\#D = 2 \mod 3$. This proves the lower bound for $n \leq 3$.
Now suppose that $n \geq 4$, and let D be a distribution with $\lceil \frac{n}{3} \rceil$ losing moves. By the proof that $\lceil \frac{n}{3} \rceil$ is the maximum number of losing moves, these must all be the same modulo 3, so there must be at least $3\lceil \frac{n}{3} \rceil - 4$ boxes (strictly) between them. We show that all of these must contain at least one ball.
Suppose for a contradiction that box d is an empty box lying between the leftmost losing move and the rightmost losing move. Then Ann has no move that removes balls from both sides of box d at the same time. Hence for any losing move m of Bill, we must have both $\#_{<d}(D + [m])$ and $\#_{>d}(D + [m])$ divisible by 3. But since there is a losing move to the left of box d (which contributes 1 to the former), as well as one to its right (which contributes 1 to the latter), this is a contradiction.
This shows that at least $3\lceil \frac{n}{3} \rceil - 4$ balls are needed (if $n \geq 3$) in order to give Bill $\lceil \frac{n}{3} \rceil$ losing moves.

Ad 2. Let D be a distribution of balls over n boxes. Here a losing move m for Bill is one such that $D + [m]$ can be written as the sum of moves of types A and B, plus at most one move of type C.
We show that the maximum number of losing moves Bill can have is n, and that the minimum number of balls Ann needs to achieve this is 1 ball if $n = 1$, and $3\lfloor \frac{n}{3} \rfloor + 4$ balls otherwise.
We first give examples that attain these bounds.
For $n = 1$, we see that $D = 1$ works, since $D + [1] = C_1$. If $n = 2$, then $D = 22$ works, since $D + [1] = B_1 + C_2$ and $D + [2] = C_1 + B_2$. If $n \geq 3$ and $n \equiv 2 \mod 3$, then $D = 031^{n-4}30$ works;

- if $i \equiv 1 \mod 3$, then $D + [i] = C_2 + B_{n-1} + 01^{i-1}0^{n-i} + 0^{i-1}1^{n-i-1}0^2$, and since $n \equiv 2$ the last two terms are sums of A_d's, by mirror symmetry, all $i \equiv 2 \mod 3$ are losing for Bill as well;
- if $i \equiv 0 \mod 3$, then $D + [i] = B_2 + B_{n-1} + C_i + 0^2 1^{i-3}0^{n-i+2} + 0^i 1^{n-i-2}0^2$, and since $n \equiv 2$ the last two terms are sums of A_d's.

Moreover, since the first and last boxes of D are empty, by removing one or both of those we get examples for all $n \geq 3$.
We show that any distribution of balls over n boxes that has n losing moves must have at least 1 ball if $n = 1$, and $3\lfloor \frac{n}{3} \rfloor + 4$ balls otherwise. We first prove the following lemma.

Lemma 1. *Let D be any distribution of balls over $n \geq 2$ boxes that has n losing moves. Then $\#D \equiv 1 \mod 3$, and some move of type C occurs in $D + [m]$ for all $m \in \{1, 2, \ldots, n\}$.*

Oplossingen

Solutions

Proof. If no move of type C occurs, then by point 1, Bill can have at most $\lceil \frac{n}{3} \rceil < n$ losing moves. Moreover, every move of types A and B contribute 3 to $\#(D+[m])$ for all $m \in \{1,2,\ldots,n\}$, and a move of type C contributes 2 to $\#(D+[m])$ for all $m \in \{1,2,\ldots,n\}$. Hence $\#D \equiv 1 \mod 3$. □

The case $n = 1$ is trivial. For $n = 2$, we note that by Lemma 1, it suffices to show that $\#D > 1$. This follows since $[1]+[2]$ cannot be written as sum of moves of types A, B, or C.
Let D be a distribution of balls over $n \geq 3$ boxes that has n losing moves. Note that by Lemma 1, it suffices to show that $\#D \geq n+2$, as $n+2 \geq 3\lfloor \frac{n}{3} \rfloor + 2$.
We first show that all boxes between 2 and $n-1$ (inclusive) contain at least one ball. Suppose for a contradiction that for some $2 \leq d \leq n-1$, box d is empty. Note that Ann still has no moves that simultaneously takes away balls from both sides of box d. Therefore $\#_{<d}(D+[1]), \#_{<d}(D+[n]), \#_{>d}(D+[1]), \#_{>d}(D+[n])$ must all be either 0 or 2 modulo 3, depending on where the move of type C comes from. Hence both $\#_{<d}D$ and $\#_{>d}D$ must both be 2 modulo 3.
For $n = 3$, note that A_1 must occur in $D+[2]$, since $B_2(2), C_2(2) > 1$ and no other moves contribute to box 2. But this implies that $\#_{<2}(D-A_1), \#_{>2}(D-A_1) \equiv 1 \mod 3$, so by the argument above, we have a contradiction.
For $n \geq 4$, the above implies that if a move $m < d$ is losing, then the pair must come from the boxes to the right of d, and vice versa. So both the part of D to the left of d and that to the right of d are instances of the situation in point 1. At least one of these instances involve at least two boxes, but this implies that Bill has winning moves, which is a contradiction. Therefore all boxes between 2 and $n-1$ (inclusive) contain a ball, so $\#D \geq n-2$.
We now take a closer look at $a_1(D), a_2(D), a_3(D)$.

Lemma 2. *Let $m \in \{1,2,\ldots,n\}$. If $i \neq j \in \{1,2,3\}$ such that $a_i(D+[m]) \equiv a_j(D+[m]) \mod 3$, then a move of the form C_z, with z congruent to the unique element of $\{1,2,3\}-\{i,j\}$ modulo 3, occurs in $D+[m]$.*

Proof. Moves of type A and B do not contribute to the difference $a_i(D+[m]) - a_j(D+[m])$ modulo 3. The move C_z contributes to the difference $a_i(D+[m]) - a_j(D+[m])$ modulo 3 if and only if $z \not\equiv i, j \mod 3$. □

Lemma 3. *Let $m \in \{1,2,\ldots,n\}$, and let C_z be a move of type C occurring in $D+[m]$. If $i \neq j \in \{1,2,3\}$ such that $a_i(D+[m]-C_z) \geq a_j(D+[m])+3$, then some move of the from B_y with $y \equiv i$ occurs in $D+[m]-C_z$.*

Proof. Moves of type A do not contribute to the difference $a_i(D+[m]-C_z) - a_j(D+[m]-C_z)$. The move B_y contributes positively to $a_i(D+[m]-C_z) - a_j(D+[m]-C_z)$ if and only if $y \equiv i \mod 3$. □

Note that two of $a_1(D)$, $a_2(D)$, $a_3(D)$ must be congruent modulo 3, since otherwise their sum must be divisible by 3, which by the above is not the case. Moreover, as their sum is 1 modulo 3, it follows that the third one must be one more than the other two, modulo 3. Now let $s, t, u \in \{1,2,3\}$ be three distinct elements such that $a_t(D) \equiv a_u(D)$ modulo 3, and $a_t(D) \geq a_u(D)$.
If $a_s(D) \geq a_u(D)+1$, then let $m \equiv t \mod 3$. Consider $D+[m]$. Then $a_s(D+[m]) \equiv a_t(D+[m]) \mod 3$, so by Lemma 2, a move of the form C_z with $z \equiv u \mod 3$ occurs in $D+[m]$. As $a_s(D+[m]-C_z) \geq a_u(D+[m]-C_z)+3$ and $a_t(D+[m]-C_z) \geq a_u(D+[m]-C_z)+3$, we see that by Lemma 3, moves of the form B_y and $B_{y'}$ with $y \equiv s \mod 3$ and $y' \equiv t \mod 3$ occur in $D+[m]-C_z$. Since $y \not\equiv m \mod 3$, it follows that $D(y) \geq 3$, and therefore that $\#D \geq n$. We also have $y' \equiv m \mod 3$, so $D(y') \geq 2$. If $n = 3,4,5$, then this implies that $\#D \geq 5 \geq 3\lfloor \frac{n}{3} \rfloor + 2$. As $\#D \equiv 1 \mod 3$, it follows that $\#D \geq 3\lfloor \frac{n}{3} \rfloor + 4$. If $n \geq 6$, then either there exists some $i \equiv t \mod 3$ with $D(i) \geq 3$, or for all $i \equiv t \mod 3$ we have $D(i) = 2$. So either way, because $n \geq 6$, we find that now $\#D \geq n+2$, as desired.
If $a_s(D) < a_u(D)+1$, then let $m \equiv s \mod 3$. Consider $D+[m]$. As $a_t(D+[m]) \equiv a_u(D+[m]) \mod 3$, we see that by Lemma 2, a move of the form C_z with $z \equiv s \mod 3$ occurs in $D+[m]$. As $a_s(D+[m]-C_z)+3 \leq a_u(D+[m]-C_z) \leq a_t(D+[m]-C_z)$, it follows by Lemma 3 that moves of the form B_y and $B_{y'}$ with $y \equiv t \mod 3$ and $y' \equiv u \mod 3$ occur in $D+[m]-C_z$. Since $y, y' \not\equiv m \mod 3$, it follows that $D(y), D(y') \geq 3$, and therefore that $\#D \geq n+2$, as desired.

Oplossingen

Solutions

Problem 2015-2/C (proposed by Hendrik Lenstra)
Let p be a prime number and let k be a positive integer. Prove that for every integer n there exist integers w, x, y, z such that

$$n \equiv w^p + x^p + y^p + z^p \mod p^k.$$

Solution We received solutions from Raymond van Bommel, Thijmen Krebs and Tejaswi Navilarekallu. All received solutions started similarly, and the first part of the following solution is based on those. The last part of the following solution is based on that of Raymond van Bommel. The book token goes to Thijmen Krebs.
For $p = 2$ this is well known; any positive integer can be written as the sum of four squares. Therefore assume p is odd. We prove by induction on k the following stronger statement.

Lemma 4. *For every integer n there exist integers w, x, y, z, with w coprime to p, such that*

$$n \equiv w^p + x^p + y^p + z^p \mod p^k.$$

Our base case is the case $k = 2$; this case automatically implies the case $k = 1$.
First note that if $n^p \equiv n \mod p^2$, then we're done; we can take $(1, -1, 0, n)$ as solution in that case. Therefore assume that $n^p \not\equiv n \mod p^2$; by Fermat's little theorem, $n - n^p$ is divisible by p, and then our assumption implies that $m = \frac{n-n^p}{p}$ is coprime to p.
Note that $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is a cyclic group of order $(p-1)p$. Therefore there exists $a \in \mathbb{Z}_{>0}$ such that $a^p \not\equiv a \mod p^2$. Let a be the smallest such positive integer and note that $a > 1$. Then $1^p + (a-1)^p + (-a)^p \equiv rp \mod p^2$ for some integer r coprime to p. So there exists an integer s coprime to p such that $m \equiv rs \mod p$, and since $s^p \equiv s \mod p$, it follows that $s^p + \big(s(a-1)\big)^p + (-sa)^p \equiv rsp \equiv mp \equiv n - n^p \mod p^2$. Hence $n \equiv s^p + \big(s(a-1)\big)^p + (-sa)^p \mod p^2 + n^p$, so $\big(s, s(a-1), -sa, n\big)$ is a solution of the desired form. This completes the base case.
As our induction hypothesis, suppose that our claim holds if $k = i \geq 2$. Then consider the case $k = i + 1$.
Suppose that n is an integer. By our induction hypothesis, there exist integers w, x, y, z, with w coprime to p, such that

$$n \equiv w^p + x^p + y^p + z^p \mod p^i.$$

Note that $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic of order $(p-1)p^{k-1}$ for all integers $k \geq 2$. Therefore the number of p-th powers in $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is equal to $(p-1)p^{k-2}$. Now note that the reduction map $(\mathbb{Z}/p^{i+1}\mathbb{Z})^\times \to (\mathbb{Z}/p^i\mathbb{Z})^\times$ that is p-to-1, and maps p-th powers to p-th powers. So comparing the number of p-th powers on each side, we see that all pre-images of p-th powers s in $(\mathbb{Z}/p^i\mathbb{Z})^\times$ are again p-th powers.
In particular, we see that $n - x^p - y^p - z^p$ defines a p-th power in $(\mathbb{Z}/p^i\mathbb{Z})^\times$, therefore also defines a p-th power in $(\mathbb{Z}/p^{i+1}\mathbb{Z})^\times$ as well, which completes the induction.