Problemen

Problem Section

Edition 2015-1 We received solutions from Rik Bos, Josse van Dobben de Bruyn, José María Giral, Alex Heinis, José Hernández Santiago, Thijmen Krebs, Robert van der Waall and Jeroen Winkel.

Problem 2015-1/A (proposed by Raymond van Bommel and Julian Lyczak)
A commutative ring R is *charming* if every ideal of R is an intersection of maximal ideals. Prove that a Noetherian charming ring is a finite product of fields. Does there exist a charming ring that is not a product of fields?

Solution We received solutions from Rik Bos, Josse van Dobben de Bruyn, José María Giral and Jeroen Winkel. The following solution is based on that of José María Giral, who also receives the book token. The example used in the following solution was given by Rik Bos, Josse van Dobben de Bruyn and José María Giral.
We first show that a Noetherian charming ring is a finite product of rings. The following lemma on general charming rings will be useful for this.

Lemma. *Let R be a charming ring. Then every prime ideal of R is maximal.*

Proof. First note that every ideal of R is an intersection of maximal — in particular radical — ideals, so every ideal of R is radical. In particular, for all $r \in R$ we have $(r^2) = (r)$, so for all $r \in R$ there exists some $s \in R$ such that $r = sr^2$.
Now let $\mathfrak{p}$ be a prime ideal of R, and let $r \in R$ be an element such that $r \notin \mathfrak{p}$. Then for $s \in R$ such that $r = sr^2$, we have $r(1 - sr) = 0 \in \mathfrak{p}$. Therefore $1 - sr \in \mathfrak{p}$, from which we deduce that $\mathfrak{p} + rR = R$, since $(1 - sr) + sr = 1$. Hence $\mathfrak{p}$ is maximal. □

Let R be a Noetherian charming ring. We show that every ideal of R is a *finite* intersection of maximal ideals. Suppose for a contradiction that not every ideal of R is a finite intersection of maximal ideals. Consider the (non-empty) collection $\mathcal{I}$ of ideals I that are not finite intersections of maximal ideals. As R is Noetherian, any ascending chain of ideals in $\mathcal{I}$ stabilises, so the union of any chain of ideals in $\mathcal{I}$ is again an ideal in $\mathcal{I}$. Therefore by Zorn's Lemma, the collection $\mathcal{I}$ contains a maximal element. Denote such an element by I.
Note that by Lemma, the ideal I is not prime. Therefore there exist $x, y \in R$ such that $x, y \notin I$ and $xy \in I$. Let $J_1 = I + xR$ and $J_2 = I + yR$. As all ideals of R are radical, we have $J_1 \cap J_2 = J_1 J_2 = xyR + xR \cdot I + yR \cdot I + I^2 = I$. By maximality of I, both J_1 and J_2 are finite intersections of maximal ideals. Therefore so is I, but this is a contradiction. So all ideals of R are finite intersections of maximal ideals.
In particular, 0 is a finite intersection of maximal ideals $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$, and maximal ideals are pairwise coprime, so by the Chinese Remainder Theorem, we have $R \cong \prod_{i=1}^{n} R/\mathfrak{m}_i$, which is a finite product of fields.
For the second part, we show that the answer to the question is yes. We first show that all *Boolean* rings — rings in which every element is an idempotent — are charming. Let R be a Boolean ring. First note that every prime ideal of R is maximal; if $\mathfrak{p} \subseteq R$ is a prime ideal and $r \in R - \mathfrak{p}$, then $r^2 = r$, so $r(1-r) = 0 \in \mathfrak{p}$, hence $1 - r \in \mathfrak{p}$ and therefore $1 = (1-r) + r \in \mathfrak{p} + rR$.
Now we note that every ideal in R is radical; if $r \in R$ such that $r^n \in I$ for some positive integer n, then $r = r^n \in I$. Therefore I is the intersection of the prime (hence maximal) ideals containing I, showing that R is charming.
Let R be the subring of $\prod_{i=1}^{\infty} \mathbb{F}_2$ consisting of the elements $(a_i)_{i=1}^{\infty}$ such that either all but finitely many a_i are zero or all but finitely many a_i are one. Note that all elements of R are idempotents, so R is Boolean, hence charming. Also, the only fields of which all elements are idempotents are isomorphic to $\mathbb{F}_2$, so all quotients of R by maximal ideals and all subfields of R are isomorphic to $\mathbb{F}_2$. So if R is a product of fields, then it must be isomorphic to a product of $\mathbb{F}_2$. Since products of $\mathbb{F}_2$ are either finite or uncountable, and since R is countable, it follows that R is not a product of fields. Therefore R is a charming ring that is not a product of fields, as desired.

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

22

Oplossingen

Solutions

Problem 2015-1/B (folklore)
Let S be a set of prime numbers with the following property: for all $n \geq 0$ and distinct $p_1, \ldots, p_n \in S$ the prime divisors of $p_1 \cdots p_n + 1$ are also in S. Show that S contains all primes.

Solution We received solutions from Thijmen Krebs and Jeroen Winkel. The following solution is based on that of Thijmen Krebs, who also receives the book token.
Fix any prime q. We say that a prime p in S is *q-recurring* if S contains infinitely many primes that are congruent to p modulo q. Note that there are only finitely many primes p in S that are not q-recurring. Let x denote the product of all primes p in S that are not q-recurring. Let y be any finite product of distinct q-recurring primes in S. Then note that all prime divisors of $xy+1$ lie in S. As $\gcd(xy+1, x) = 1$, it follows by definition of x that moreover all prime divisors of $xy+1$ are q-recurring.
We can now define a sequence $(y_i)_{i=0}^{\infty}$ of products of q-recurring primes recursively by setting $y_0 = 1$, and by setting for $n \geq 1$ the number y_n to be the number obtained from $xy_{n-1}+1$ in the following way. Let $p_1 p_2 \cdots p_s$ be the prime factorisation of $xy_{n-1}+1$ (in which primes can occur multiple times). Pick for each p_i a prime p_i' in S that is congruent to p_i modulo q, in such a way that all p_i' *are* distinct; this is possible as there are infinitely many such p_i'. Then set $y_n = p_1' p_2' \cdots p_s'$. An inductive argument quickly shows that for all non-negative integers n, we have
$$y_n \equiv x^n + \cdots + x + 1 \mod q.$$
We now show that $q \in S$. If $x \equiv 0$ modulo q, then $q \in S$ by definition of x. If $x \equiv 1$ modulo q, then by the above we conclude that $q \mid y_{q-1}$ so $q \in S$ by definition of y_{q-1}. Finally, in the other cases, we can apply Fermat's Little Theorem to see that since $(x-1)y_{q-2} \equiv x^{q-1} - 1$ modulo q, we have $q \mid y_{q-2}$, so $q \in S$ by definition of y_{q-2}. Therefore $q \in S$, as desired.

Problem 2015-1/C (proposed by Roberto Stockli)
Determine all pairs (p, q) of odd primes with $q \equiv 3 \mod 8$ such that $\frac{1}{p}(q^{p-1} - 1)$ is a perfect square.

Solution We received solutions from Alex Heinis, José Hernández Santiago, Thijmen Krebs, Robert van der Waall and Jeroen Winkel. The following solution is based on that of Alex Heinis, who also receives the book token. In addition, we thank Robert van der Waall for bringing our attention to the article [1], in which one of the results is that the equation $\frac{1}{p}(m^{p-1} - 1) = a^2$ has a unique integral solution $(m, p, a) = (3, 5, 4)$ with m odd.
Note that $(p, q) = (5, 3)$ is a solution. We show that it is the only one.
Suppose that (p, q) is a solution. Then $(q^{(p-1)/2} + 1)(q^{(p-1)/2} - 1)/p$ is a square. Both factors on the left hand side are even as q is odd, so their greatest common divisor is 2. Therefore the two factors are of the forms $2a$ and $2pb$ for certain positive integers a, b, in no particular order, such that $\gcd(a, pb) = 1$. As ab is a square, it follows that both a and b are squares. Note that 2 is not a square modulo q as $q \equiv 3$ modulo 8. Therefore $q^{(p-1)/2} + 1$ cannot be twice a square. It follows that $q^{(p-1)/2} - 1$ is twice a square.
Hence $q^{(p-1)/2} - 1 = 2a$ and $q^{(p-1)/2} + 1 = 2pb$. Writing $a = k^2$ and $b = l^2$ for integers k, l, we can rewrite the above system of equations as $q^{(p-1)/2} = k^2 + pl^2$ and $1 = pl^2 - k^2$. Note that precisely one of k and l is even as precisely one of $q^{(p-1)/2} - 1$ and $q^{(p-1)/2} + 1$ is divisible by 4. If l were even, then $1 \equiv -k^2$ modulo 4, which is a contradiction. So l is odd, k is even, and therefore $p \equiv 1$ modulo 4. Hence we have a factorisation $(q^{(p-1)/4} + 1)(q^{(p-1)/4} - 1)$ of $2k^2$ with integer factors.
In the same way as above, we see that the two factors on the left hand side are of the forms $2c^2$ and $4d^2$ for certain positive integers c, d, in no particular order, and that $q^{(p-1)/4} + 1$ cannot be twice a square. Therefore we write $q^{(p-1)/4} - 1 = 2c^2$ and $q^{(p-1)/4} + 1 = 4d^2$. Hence $q^{(p-1)/4} = (2d-1)(2d+1)$. Note that $\gcd(2d-1, 2d+1) = 1$. As q is prime, it follows that since d is positive, we must have $2d - 1 = 1$, so $d = 1$. Hence $q = 3$ and $p = 5$. This shows that $(p, q) = (5, 3)$ is the only solution.

Reference
1. Hiroyuki Osada, Nobuhiro Terai, *Generalization of Lucas' Theorem for Fermat's quotient*, Comptes Rendus de Mathématiques de l'Académie des Sciences 01/1989; 11(4).