The Divisibility Poset inside Itself: 10623

Roy Barbara; Nasha Komanda; Robin J. Chapman

The American Mathematical Monthly, Vol. 106, No. 9. (Nov., 1999), pp. 868-869.

(a_n, b_n, c_n) meets the conditions of the problem. By the recurrence, $c_n - b_n = b_n - a_n$, and we have arithmetic progressions.

To prove that $a_n c_n + 1$ is a perfect square, we prove by induction on n that $a_n a_{n+2} + 1 = a_{n+1}^2$. For $n = 0$, we have $1 \cdot 15 + 1 = 4^2$. For $n > 0$, we use the recurrence and the induction hypothesis to compute

$$a_n a_{n+2} + 1 = 4a_n a_{n+1} - a_n^2 + 1 = 4a_n a_{n+1} - a_{n-1}a_{n+1} = a_{n+1}^2.$$

Next, we use this formula and the recurrence to compute

$$a_n b_n + 1 = 2a_n a_{n+1} + 1 = 2a_n a_{n+1} + a_{n+1}^2 - a_n a_{n+2} = a_{n+1}^2 - a_n(a_{n+2} - 2a_{n+1})$$
$$= a_{n+1}^2 - a_n(2a_{n+1} - a_n) = (a_{n+1} - a_n)^2.$$

Similarly $b_n c_n + 1 = (a_{n+2} - a_{n+1})^2$, so all desired properties hold.

Solution II by Zachary Franco, Butler University, Indianapolis, IN. In $\mathbb{Z}[\sqrt{3}]$, the norm $\|r + s\sqrt{3}\| = r^2 - 3s^2$ is multiplicative and satisfies $\|2 + \sqrt{3}\| = 1$. Therefore, $\|(2 + \sqrt{3})^n\| = 1$. For the expansion $(2 + \sqrt{3})^n = r + s\sqrt{3}$, we thus have

$$3s^2 = r^2 - 1. \qquad (*)$$

For $n > 1$, the triple $(a, b, c) = (2s - r, 2s, 2s + r)$ is in arithmetic progression and satisfies $(2s - r)2s + 1 = (r - s)^2$, $(2s - r)(2s + r) + 1 = s^2$, and $2s(2s + r) + 1 = (r + s)^2$.

Editorial comment. The two solutions generate the same family of triples. Jan Kristian Haugland, John P. Robertson, and Ivan Vidav independently proved that this family contains all triples with $a \le b \le c$ that satisfy the conditions of the problem. Betsy Carper, Gary Hull, Lenny Jones, and Bonnie Wachhaus observed that for each triple in this family there is no fourth integer d such that a, b, c, d are in arithmetic progression and both $bd + 1$ and $cd + 1$ are perfect squares. Hence there is no quadruple of positive integers in arithmetic progression such that $ij + 1$ is a perfect square for all i, j in the quadruple.

David M. Bloom observed that this problem is related to problem 10238 [1992, 674; 1995, 275]. The published solution for that problem used the Pell equation $(*)$.

Solved also by I. Adler, M. Aissen, J. Anglesio (France), B. D. Beasley, J. C. Binz (Switzerland), D. M. Bloom, J. Bowring, J. T. Bruening, S. Byrd, R. J. Chapman (U. K.), J. Christopher, C. R. Diminnie, R. DiSario, H. Y. Far, J. K. Haugland (Norway), R. Heller, L. Jones et al., N. Komanda, J. Lee, N. F. Lindquist, C. Mack, L. G. Mans, A. S. Mittal, G. R. Mott, Y. Pan, M. Reekie, J. P. Robertson, H. Sedinger, N. C. Singer, W. R. Smythe, P. Trajovský (Czech Republic), I. Vidav (Slovenia), M. Vowe (Switzerland), X. Wang, C. H. Webster, P. Yiu, Anchorage Math Solutions Group, GCHQ Problems Group (U. K.), NSA Problems Group, NCCU Problems Group, SAS Maths Club (India), WMC Problems Group, and the proposer.

The Divisibility Poset Inside Itself

10623 [1997, 870]. *Proposed by Roy Barbara, Lebanese University, Fanar, Lebanon.* Let $P = \{1, 2, 3, \ldots\}$, and let $|$ be the usual divisibility relation on P. For any $S \subseteq P$ and $n \in P$, let $S + n = \{s + n : s \in S\}$.

(**a**) Can one construct a subset S of P such that the poset $(S, |)$ is isomorphic to $(P, |)$, $(S + 1, |)$ is isomorphic to $(P, \le)$, and $(S + 2, |)$ is isomorphic to $(P, |)$?

(**b**) For which integers $n \ge 1$ can one find a subset T of P such that $(T, |)$, $(T + n, |)$, and $(P, |)$ are isomorphic posets?

Solution to (**a**) *by Nasha Komanda, Central Michigan University, Mt. Pleasant, MI.* The answer is yes. First we prove for positive integers x, y and for integers $a \ne \pm 1$ that

$$\gcd(a^x - 1, a^y - 1) = |a^{\gcd(x,y)} - 1|. \qquad (*)$$

We may assume that $x \ge y$. From $a^x - 1 = a^{x-y}(a^y - 1) + (a^{x-y} - 1)$ we obtain $\gcd(a^x - 1, a^y - 1) = \gcd(a^y - 1, a^{x-y} - 1)$. Also $\gcd(x, y) = \gcd(y, x - y)$. Thus $(*)$ follows by induction on $x + y$. If also x and y are odd, then

$$\gcd(a^x + 1, a^y + 1) = \gcd((-a)^x - 1, (-a)^y - 1) = |(-a)^{\gcd(x,y)} - 1| = |a^{\gcd(x,y)} + 1|.$$

For positive integers a, x, y with $a > 1$, it follows that $(a^x - 1)|(a^y - 1)$ if and only if $x|y$. When x and y are odd, we also have $(a^x + 1)|(a^y + 1)$ if and only if $x|y$.

Now let $S = \{2^{2^x - 1}: x \in P\}$. For $x, y \in P$,

$$(2^{2^x-1} - 1)|(2^{2^y-1} - 1) \iff (2^x - 1)|(2^y - 1) \iff x|y.$$

Thus $(S, |)$ is isomorphic to $(P, |)$. Also

$$(2^{2^x-1})|(2^{2^y-1}) \iff (2^x - 1) \le (2^y - 1) \iff x \le y.$$

Thus $(S + 1, |)$ is isomorphic to $(P, \le)$. Since $2^x - 1$ and $2^y - 1$ are odd, we have

$$(2^{2^x-1} + 1)|(2^{2^y-1} + 1) \iff (2^x - 1)|(2^y - 1) \iff x|y.$$

Thus $(S + 2, |)$ is isomorphic to $(P, |)$.

Solution to (**b**) *by Robin J. Chapman, University of Exeter, Exeter, U. K.* Such a T exists for all $n \in P$. Let $O = \{1, 3, 5, \ldots\}$ be the set of odd positive integers. Let p_j denote the j-th smallest prime. Then $\phi : \prod_j p_j^{r_j} \to \prod_j p_{j+1}^{r_j}$ is an isomorphism from $(P, |)$ to $(O, |)$.

Given $n \in P$, let $T = nO = \{nm : m \in O\}$. Then $T + n = 2nP = \{2nk : k \in P\}$. The posets $(T, |)$ and $(O, |)$ are isomorphic, and $(T + n, |)$ and $(P, |)$ are isomorphic. We obtain $(T, |)$ isomorphic to $(T + n, |)$ by transitivity.

Part (**a**) solved also by R. J. Chapman (U. K.). Both parts solved also by J. Dawson (Australia), GCHQ Problems Group (U. K.), and the proposer.

An Equation Involving the Totient

10626 [1997, 871]. *Proposed by Florian Luca, Syracuse University, Syracuse, NY.* For a positive integer k, the number of positive integers less than k that are relatively prime to k is denoted $\phi(k)$.

(**a**) Show that if m and n are relatively prime positive integers, then $\phi(5^m - 1) \neq 5^n - 1$.

(**b**)* Find all positive integers m, n such that $\phi(5^m - 1) = 5^n - 1$.

Solution to (**a**) *by Nasha Komanda, Central Michigan University, Mt. Pleasant, MI.* We use the lemma proved in Problem **10623**: $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$ when a, m, n are positive integers.

When $\gcd(m, n) = 1$, the lemma yields $\gcd(5^m - 1, 5^n - 1) = 4$. When $5^m - 1$ has the prime factorization $2^{e_0} \prod_{i=1}^s p_i^{e_i}$ with all exponents positive, we have $\phi(5^m - 1) = 2^{e_0 - 1} \prod_{i=1}^s p_i^{e_i - 1}(p_i - 1)$. Suppose that $\phi(5^m - 1) = 5^n - 1$. Since $\gcd(5^m - 1, 5^n - 1) = 4$, we have $e_i = 1$ for $1 \le i \le s$.

If m is even, then $5^m - 1 = 25^{m/2} - 1$ is divisible by 8. Therefore, $e_0 \ge 3$. Since m and n are relatively prime, n is odd, so $5^n - 1 \equiv 4 \pmod 8$, which implies that $e_0 - 1 + s \le 2$. Thus $e_0 = 3$ and $s = 0$, which yields the impossibility $5^m - 1 = 8$.

Thus m is odd, which yields $e_0 = 2$. Since $e_i = 1$ for $1 \le i \le s$, we have $5^m - 1 = 4 \prod_{i=1}^s p_i$. Thus $5^m \equiv 1 \pmod{p_i}$ for $1 \le i \le s$. Since m is odd, 5 is a quadratic residue modulo p_i. By the Quadratic Reciprocity Law, each p_i is a quadratic residue modulo 5. Thus $p_i \equiv \pm 1 \pmod 5$. If $p_i \equiv 1 \pmod 5$, then $p_i - 1 \equiv 0 \pmod 5$ and $5^n - 1 \equiv 0 \pmod 5$, which is impossible. Therefore, $p_i \equiv -1 \pmod 5$ for $1 \le i \le s$. Our formula for $5^m - 1$ now yields $-1 \equiv (-1)^{s+1} \pmod 5$, and hence s is even.

On the other hand, $e_i = 1$ for $1 \le i \le s$ also yields $5^n - 1 = 2 \prod_{i=1}^s (p_i - 1)$. With $p_i \equiv -1 \pmod 5$, this yields $-1 \equiv 2(-2)^s \pmod 5$. This requires $s \equiv 3 \pmod 4$, which contradicts our conclusion that s is even. Thus m can be neither odd nor even, and no solution exists.

Editorial comment. No solution was received to part (**b**). Roy Barbara provided partial results about the general equation $\phi(a^m - 1) = a^n - 1$, with additional partial results in