Solutions to AMM problems 11628, 11631, and 11636

TCDmath problem group
*Mathematics, Trinity College, Dublin 2, Ireland**

July 12, 2012

1 AMM problem 11628

Solvers: TCDmath problem group, Mathematics, Trinity College, Dublin 2, Ireland.

The *Lenstra number* of a commutative unital ring R is the maximum cardinality of all sets A with the property that for every pair $a, b \in A$, if $a \neq b$ then $a - b$ is invertible. Show that when $R = \mathbb{Z}[1/N]$, where N is a positive integer, the Lenstra number of R is the smallest prime p not dividing N.

Answer. Elements of R can be written as x/N^r where $x \in \mathbb{Z}$ and $r \geq 0$. If

$$\frac{x}{N^r}\frac{y}{N^s} = 1$$

then xy is a nonnegative power of N, whence x and y both divide sufficiently high powers of N, and it follows that x/N^r is invertible, where $x \neq 0$, if and only if every prime dividing x also divides N.

Let $A = \{0, \ldots, p-1\}$. Given $a \neq b \in A$, $|b-a| < p$, so every prime dividing $a-b$ also divides N, so $a - b$ is invertible. This shows that p is a lower bound for the Lenstra number.

Let B be any subset of R with $|B| > p$. Claim that for some $a \neq b \in B$, $a - b$ is not invertible. Since if z is invertible then so is zN^t for any t, we can assume that $B \subseteq \mathbb{Z}$. But $|B| > p$, so there exist $a \neq b \in B$ so that $a \equiv b \pmod{p}$. Then p divides $a - b$, so $a - b$ is not invertible. This shows that p is an upper bound for the Lenstra number. ∎

*This group involves students and staff of the Department of Mathematics, Trinity College, Dublin. Please address correspondence either to Timothy Murphy (`tim@maths.tcd.ie`), or Colm Ó Dúnlaing (`odunlain@maths.tcd.ie`).

2 AMM problem 11631

Solvers: TCDmath problem group, Mathematics, Trinity College, Dublin 2, Ireland.

A *quasigroup* Q is a (nonempty) set with a binary operation $x \times y$

(a) which is left and right cancellative.

Equivalently, in its Cayley table, every row and column defines a permutation. Say a Cayley table has property P if

(b) all rows are cyclic shifts of one another,

and

(c) every element is an idempotent.

Question: for which n does there exist a P-quasigroup of order n?

Answer: (d) n admits such a quasigroup iff n is odd.

To show this, we assume that the Cayley tables have elements $\{1, \ldots, n\}$ and the i, j entry is $i \times j$. Congruence mod n is denoted $\equiv_n$.

We identify the i-th row with the permutation $j \mapsto i \times j$, and let π represent the top row, i.e., $j \mapsto 1 \times j$. Assuming (b), the i-th row is a cyclic shift of the first, by a shift of g_i places, say. For (c), writing 'i Mod n' for $((i-1) \mod n) + 1$,

$$i \times i = i \iff \pi((i + g_i) \text{ Mod } n) = i \iff g_i \equiv_n \pi^{-1}(i) - i.$$

We now assume (b) and (c), so $g_i \equiv_n \pi^{-1}(i) - i$, and every row has distinct elements. Assuming (b) and (c), **claim:** (a) holds iff all g_i are distinct modulo n.

If they are not distinct modulo n, so $g_i \equiv_n g_j$ where $i \neq j$, then $\pi(j + g_i) = \pi(j + g_j) = j$, and j occurs in the j-th column at positions i and j, so (a) does not hold.

If they are distinct modulo n, then every column is a permutation of the first row, hence of $\{1, \ldots, n\}$, with distinct elements, so (a) holds, proving the claim.

Proof of (d):

Given n is odd, consider the Cayley table whose top row is $1, n, n-1, \ldots, 3, 2$, and with properties (b) and (c). If $i > 1$ then $\pi(i) = \pi^{-1}(i) = n + 2 - i \equiv_n 2 - i$, also valid for $i = 1$, and $\pi^{-1}(i) - i \equiv_n 2 - 2i$. Since n is odd, for $1 \leq i \leq n$ these numbers are distinct modulo n, and (a) holds: we have a P-quasigroup.

Given n is even, and assuming (b) and (c), we consider

$$\sum_i g_i \equiv_n \sum_i (\pi^{-1}(i) - i) \equiv_n n(n+1)/2 - n(n+1)/2 \equiv_n 0$$

Claim that the g_i cannot all be distinct (modulo n). Otherwise, $\sum_i g_i \equiv_n n(n-1)/2$. But if n is even, then the highest power of 2 dividing n does not divide $n(n-1)/2$, so $n(n-1)/2 \not\equiv_n 0$ and (a) cannot hold. ∎

3 AMM problem 11636

Solvers: TCDmath problem group, Mathematics, Trinity College, Dublin 2, Ireland.

Given a convex quadrilateral $ABCD$, suppose there exists a point M on the diagonal BD such that the following triangle perimeter lengths are equal (in length):[1]

$$\Delta ABM = \Delta BCM \quad \text{and} \quad \Delta AMD = \Delta MCD. \tag{3.1}$$

Prove that

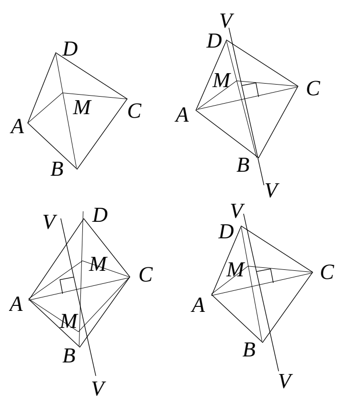
$$|AB| = |BC| \quad \text{and} \quad |AD| = |CD|. \tag{3.2}$$

Equivalently, we suppose (3.2) false and deduce that (3.1) is false. We consider the position of M relative to the perpendicular bisector V of AC. Also, we consider three cases separately. Without loss of generality, $|AB| \leq |BC|$.

Case 1: one pair equal; wlog $|AB| = |BC|$ and $|AD| < |CD|$. The bisector V passes through B and M must be to the left of V. Then $|AM| < |MC|$, so $\Delta ABM < \Delta BCM$.

Case 2: $|AB| < |BC|$ and $|AD| > |CD|$. In this case V intersects the diagonal BD. If M is below this intersection, then $|AM| < |MC|$ so $\Delta ABM < \Delta BCM$. If M is above, then $|AM| > |MC|$ so $\Delta AMD > \Delta MCD$.

Case 3: $|AB| < |BC|$ and $|AD| < |CD|$. Then M is always to the left of V, and $\Delta ABM < \Delta BCM$. ∎



[1] We use ΔABC to denote $|AB| + |BC| + |CA|$.