On the spur of the moment we also talked about an additional problem from an old Putnam exam, that was kind of Abstract-Algebra-y.

Suppose $*$ is a binary operation on a set S, and satisfies the conditions
for all $x, y \in S$, we have $x * (x * y) = y$; and
for all $x, y \in S$, we have $(y * x) * x = y$
Then show this binary operation is commutative. Show also that it need not be associative.

For any two elements $a, b \in S$ we can use the two properties to rewrite

$$a * ((b * (b * a)) * (b * a))$$

in two ways: First use the second axiom with $x = b * a$ and $y = b$ to conclude this is $a * b$. On the other hand we can use the first axiom (first with $x = b, y = a$) to rewrite it as $a * (a * (b * a))$, and then use the axiom again (now with $x = a, y = b * a$) to rewrite it as $b * a$. This shows $a * b = b * a$. Since this is true for all a and b in S, the operation is commutative.

We remark that in the presence of commutativity, the two axioms are now seen to be redundant.

Note that if the operation *were* associative, we would conclude that $a*a = a*((a*b)*b)$ and $b*b = (a*(a*b))*b$, were equal, i.e.every element would have the same square. Denoting this common square by e, we would have $e * a = (e * e) * a = e * (e * a) = a$ and likewise $a * e = a$; so e serves as a two-sided identity element. Since $a * a = e$, every element has an inverse (namely itself). Thus if the operation were associative, then $(S, *)$ would be an abelian group. (It would have exponent 2 since $a^2 = e$ for every a.) In particular if S were a finite set, then its cardinality would be a power of 2 by Lagrange's Theorem (indeed, S would be isomorphic to Z_2^n for some n).

So when we search for non-associative examples, we look first at sets S whose cardinality is not a power of 2. And indeed, we can construct such examples with $|S| = 3$. For example, this multiplication table is easily seen to satisfy the two axioms (and is indeed commutative)

	a	b	c
$a:$	a	c	b
$b:$	c	b	a
$c:$	b	a	c

For further examples, we may also use the groups suggested by this analysis: if $(S, *)$ is an abelian group of exponent 2, then the two initial axioms are satisfied.