THEOREM OF THE DAY

The Lagrange Property for Moufang Loops *If M is a finite Moufang loop then M has the Lagrange Property: the order of any subloop divides the order of M.*

$*$	K	E	D	W	L
K	K	E	D	W	L
E	E	K	W	L	D
D	D	L	K	E	W
W	W	D	L	K	E
L	L	W	E	D	K

A *quasigroup* is a set Q with a multiplication operation $*$ whose multiplication table has each element of Q exactly once in each row and column. This makes the table precisely a Latin square. Suppose that the first row and column of the table are identical to the row and column labels, respectively, as is the case with the tables above and to the right. This means that the first label in each case is an *identity element*: it is an element which leaves everything unchanged by multiplication. A quasigroup with identity is a *loop*.

$*$	1	a	b	c	d	e	u	v	w	x	y	z
1	1	a	b	c	d	e	u	v	w	x	y	z
a	a	1	d	e	b	c	v	u	y	z	w	x
b	b	e	1	d	c	a	w	z	u	y	x	v
c	c	d	e	1	a	b	x	y	z	u	v	w
d	d	c	a	b	e	1	y	x	v	w	z	u
e	e	b	c	a	1	d	z	w	x	v	u	y
u	u	v	w	x	z	y	1	a	b	c	e	d
v	v	u	y	z	x	w	a	1	e	d	b	c
w	w	z	u	y	v	x	b	d	1	e	c	a
x	x	y	z	u	w	v	c	e	d	1	a	b
y	y	x	v	w	u	z	d	b	c	a	1	e
z	z	w	x	v	y	u	e	c	a	b	d	1

The Moufang loop M(S_3, u)

Now, a loop that is associative is a *group* and satisfies Lagrange's Theorem: any subgroup has order dividing the order of the group. But loop multiplication will not normally be associative. We can read off, for example, from the left-hand table, that $(E * D) * L = W * L = E \neq L = E * W = E * (D * L)$. Non-associativity can suffice to destroy the Lagrange property; indeed, we see immediately from the left-hand table that any element, taken with the identity K, forms a two-element subloop; and certainly two does not divide five! The right-hand table, on the other hand, represents the loop $M(S_3, u)$, which satisfies the identity $x(y(xz)) = ((xy)x)z$ (a weak version of associativity) and is therefore a *Moufang loop*. With order 12 it is the smallest Moufang loop that is non-associative. It has subloops with orders precisely 1, 2, 3, 4, and 6.

Moufang loops arose out of work by Ruth Moufang in the 1930s on coordinatisation of projective planes. Whether they have the Lagrange property was an open question for over forty years. It was solved in 2003, assuming the classification of the finite simple groups, by Alexander N. Grishkov and Andrei V. Zavarnitsine, and independently, in 2004, by Stephen M. Gagola III and Jonathan I. Hall, who acknowledge yet a third independent and, more or less, simultaneous proof by G. Eric Moorhouse!

Web link: arxiv.org/abs/math/0205141, just predating this theorem, nevertheless remains an excellent introduction. The instructions for constructing $M(G, u)$ from a group G, due to Orin Chein in 1974, are here: en.wikipedia.org/wiki/Moufang_loop#Examples

Further reading: *Theory of Groups* by Marshall Hall, MacMillan, New York, 1959, chapter 20.