Construction of latin squares of prime order

Theorem. If p is prime, then there exist $p-1$ MOLS of order p.

Construction: The elements in the latin square will be the elements of $\mathbb{Z}_p$, the integers modulo p. Addition and multiplication will be modulo p.

Choose a non-zero element $m \in \mathbb{Z}_p$. Form L^m by setting, for all $i, j \in \mathbb{Z}_p$,

$$L^m_{i,j} = mi + j.$$

Claim: L^m is a latin square.

No two elements in a column are equal: Suppose $L^m_{i,j} = L^m_{i',j}$. Then $mi + j = mi + j'$, so $j = j'$.

No two elements in a row are equal: Suppose $L^m_{i,j} = L^m_{i,j'}$. Then $mi + j = mi' + j$, so $(i - i')m = 0$ (modulo p). Since p is a prime, this implies $i = i'$.

Construction of latin squares of prime order

Choose a non-zero element $m \in \mathbb{Z}_p$. Form L^m by setting, for all $i, j \in \mathbb{Z}_p$,

$$L^m_{i,j} = mi + j.$$

Claim: If $m \neq t$, then L^m and L^t are orthogonal.

Suppose a pair of entries occurs in location (i, j) and location (i', j'). So $(L^m_{i,j}, L^t_{i,j}) = (L^m_{i',j'} = L^t_{i',j'})$. Then $mi + j = mi' + j'$ and $ti + j = ti' + j'$. So $(m - t)(i - i') = 0$. Since $m \neq t$ and p is prime, this implies that $i = i'$. It follows that $j = j'$.

Construction of latin squares from finite fields

We can use the same construction to find two MOLS of order n if we have a **field** of order. A field consists of a set and two operations, multiplication and addition, which satisfy a set of axioms.

As an example, $\mathbb{Z}_p$ equipped with multiplication and addition modulo p is a field.

The axioms require that there is an identity element for addition (usually denoted by 0), and for multiplication (denoted by 1).

The important property for our construction is that in a field, for any two elements x, y, then

$$xy = 0 \quad \Rightarrow \quad x = 0 \text{ or } y = 0.$$

Using this property it follows from that previous proof that, for a field of size n, the construction of $n-1$ MOLS as given earlier works as well.

Finite fields

A famous theorem of Galois states that finite fields of size n exist if and only if $n = p^k$ for some prime p, positive integer k. Such fields have a special form:

- Elements: polynomials of degree less than k with coefficients in $\mathbb{Z}_p$
- Addition is modulo p, 0 is the additive identity.
- Multiplication is modulo p, and modulo an *irreducible polynomial* of degree k. This polynomial essentially tells you how to replace the factors x^k that arise from multiplication.

An irreducible polynomial is a polynomial that cannot be factored.

Finite fields: an example

Consider the following field of order 4.

- Elements: polynomials of degree less than 2 with coefficients in $\mathbb{Z}_2$. This field has 4 elements: $\{0, 1, x, 1+x\}$.

- Multiplication: Modulo 2, and modulo the polynomial $f(x) = 1 + x + x^2$ This implies that $1+x+x^2 = 0 \pmod{f(x)}$, and thus $x^2 = -x-1 = x+1$ (Note that $-1 = 1 \mod 2$).

The tables for addition and multiplication are as follows.

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	1	x	$1+x$
1	1	x	$1+x$
x	x	$1+x$	1
$1+x$	$1+x$	1	x

We can use these to construct three MOLS L^1, L^x and L^{1+x}.

Construct large MOLS from small

Given two latin squares L, of size $n \times n$, and M, of size $m \times m$.

Define an $nm \times nm$ square $L \oplus M$ as follows.

For all $0 \leq i, k < n$ and $0 \leq j, \ell < m$, let

$$(L \oplus M)_{mi+j, mk+\ell} = mL_{i,k} + M_{j,\ell}.$$

Thus, $L \oplus M$ consists of $n \times n$ blocks of size $m \times m$ each. All blocks have the same structure as M, but with disjoint sets of symbols. Block (i, j) uses the symbols $mL_{i,j}, \ldots, mL_{i,j} + m - 1$.

Claim: $L \oplus M$ is a latin square.

Since M is a latin square, the same element does not occur twice in a row or column of a block. Since L is a latin square, a set of symbols is only used once in each row or columns of blocks. Thus the same element cannot occur in two different blocks in the same row or column.

Construct large MOLS from small

For all $0 \leq i, k < n$ and $0 \leq j, \ell < m$, let

$$(L \oplus M)_{mi+j, mk+\ell} = mL_{i,k} + M_{j,\ell}.$$

Theorem: If L^1, L^2 are MOLS of order n, and M^1, M^2 are MOLS of order m, then $L^1 \oplus M^2$ and $L^2 \oplus M^2$ are MOLS of order nm.

Suppose the same pair appears twice, so

$(L^1 \oplus M^1)_{s,t} = (L^2 \oplus M^2)_{s,t}$ and $(L^1 \oplus M^1)_{s',t'} = (L^2 \oplus M^2)_{s',t'}$.

Suppose $s = mi + j$, $s' = mi' + j'$, $t = mk + \ell$, $t' = mk' + \ell'$, $0 \leq j, j', \ell, \ell' < m$. Then

$mL^1_{i,k} + M^1_{j,\ell} = mL^2_{i,k} + M^2_{j,\ell}$ and $mL^1_{i',k'} + M^1_{j',\ell'} = mL^2_{i',k'} + M^2_{j',\ell'}$

$mL^1_{i,k} + M^1_{j,\ell} = mL^2_{i,k} + M^2_{j,\ell}$ and $mL^1_{i',k'} + M^1_{j',\ell'} = mL^2_{i',k'} + M^2_{j',\ell'}$

Since all elements of M^1 and M^2 are smaller than m,

$mL^1_{i,k} + M^1_{j,\ell} = mL^2_{i,k} + M^2_{j,\ell}$ implies that $L^1_{i,k} = L^2_{i,k}$ and $M^1_{j,\ell} = M^2_{j,\ell}$.
$mL^1_{i',k'} + M^1_{j',\ell'} = mL^2_{i',k'} + M^2_{j',\ell'}$ implies that $L^1_{i',k'} = L^2_{i',k'}$ and $M^1_{j',\ell'} = M^2_{j',\ell'}$.

Since L^1, L^2 are MOLS, this implies that $i = i'$ and $k = k'$.
Since M^1, M^2 are MOLS, this implies that $j = j'$ and $\ell = \ell'$.

Corollary: If $n \neq 2 \mod 4$, then there exist at least two MOLS of order n.