Slide 1

Probably you have seen **Su Doku** puzzles like this one:

The Times, 14 September 2005

Rating: Fiendish

					2		4	8
						2	9	
		1	9					
1				9	5	3		
		3				4		
		8	3	1				6
					8	7		
	1	5						
2	3		5					

Slide 2

Here is the solution:

3	5	9	7	6	2	1	4	8
7	8	6	4	5	1	2	9	3
4	2	1	9	8	3	6	7	5
1	4	2	6	9	5	3	8	7
5	6	3	8	2	7	4	1	9
9	7	8	3	1	4	5	2	6
6	9	4	1	3	8	7	5	2
8	1	5	2	7	6	9	3	4
2	3	7	5	4	9	8	6	1

Slide 3

Latin squares

You see that

- each number in the puzzle occurs in the same position in the solution (that is, we just write numbers in blank squares);
- every row, column, or 3×3 subsquare of the solution contains the numbers 1 to 9 each once.

The second condition is almost the same as something that mathematicians have studied for hundreds of years: *Latin squares.* A Latin square of order n is an $n \times n$ array containing the numbers $1, \ldots, n$ in such a way that each number occurs once in each row and once in each column.

The entries of a Latin square don't have to be numbers; any symbols will do. The next slide shows a 26×26 Latin square using the letters of the alphabet.

Slide 4

Vigenère square

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Slide 5

Caesar cipher

Julius Caesar used a simple cipher to encrypt his messages. He wrote out the message, and then replaced each letter with the one three steps on in the alphabet. Thus the message

`SEND THE LEGION AT ONCE`

would be encrypted as

`VHQG WKH OHJLRQ DW RQFH`

The alphabet “wraps round”: that is, the letters `XYZ` are encrypted as `ABC`. The decryption is done by shifting back three places.
This cipher encrypts `A` as `D`. If we look at the row labelled `D` in the Vigenère square, we see that it can be used for the encryption.

Slide 6

Vigenère cipher

The Caesar cipher is not very secure; it is easy to break by trial and error.
A much better cipher, which was used for diplomatic ciphers in Europe for hundreds of years, is the *Vigenére cipher*. Choose a keyword, let us say `FOXES`. Now, using the Vigenère square, we encrypt the first letter of the message with row `F`, the second with `O`, . . . , the fifth with `S`, the sixth with `F` again, and so on, repeating the keyword as often as necessary.
Thus the message

`SEND THE LEGION AT ONCE`

would be encrypted as

`XSKH LMS IIYNCK WS YCKG`

To further confuse things, the cipher can be broken into blocks of a standard length: for example `XSKH LMSI IYNC KWSY CKGQ`, where we use blocks of four, and add a dummy letter at the end to complete the last block.

Slide 7

One-time pad

The advantage of the Vigenère cipher is that only one keyword has to be remembered by sender and receiver. But this is also its weakness, and in the nineteenth century a method of breaking it was discovered by several people, including the computer pioneer Charles Babbage.
To make a completely secure cipher, we can use the principle of the Vigenère cipher, but instead of using a word for the key, we use a random string of letters as long as the message. (The key should be truly random, not just “pseudo-random” output from a computer.)
Claude Shannon showed that this cipher is unbreakable if properly used.

Slide 8

Random Latin square

No cipher is reallly secure, since it is always possible that the enemy get hold of the key. One further refinement to the Vigenère method is to replace the Vigenère square by an arbitrary Latin square which can be changed from week to week.

We can't choose a random Latin square just by putting entries anywhere and trying to complete it: we might get stuck, and some squares might be more likely than others. A good method has been proposed by Jacobson and Matthews, using the method of *Markov chains* from probability theory.

An example is shown on the next slide.

Slide 9

A random Latin square

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	I	Z	W	O	F	X	B	N	E	D	R	L	G	Q	U	C	K	M	V	Y	H	P	J	T	S
b	Y	L	R	U	T	H	D	Z	W	X	S	J	B	C	F	V	K	M	E	Q	G	I	N	P	O	A
c	X	O	B	Y	P	S	U	A	G	J	Z	E	C	F	H	D	N	I	K	W	Q	R	V	L	M	T
d	J	H	P	S	A	X	Y	K	L	Z	M	N	I	O	R	Q	V	D	F	T	B	C	W	G	U	E
e	G	B	E	Q	R	T	Z	F	H	Y	O	C	J	X	V	M	L	U	N	S	K	A	I	W	D	P
f	C	J	Q	F	K	O	H	V	U	D	T	G	R	A	Y	B	E	P	Z	L	N	X	S	M	W	I
g	N	K	D	O	F	U	P	S	A	B	W	V	G	Z	M	L	X	Q	T	E	C	J	Y	R	I	H
h	H	G	I	C	E	A	K	R	J	Q	L	O	N	S	B	W	Z	X	D	Y	F	V	M	T	P	U
i	W	M	S	A	D	Z	T	U	Q	R	X	B	P	E	O	F	G	Y	I	J	H	N	K	C	L	V
j	Q	E	K	L	G	B	M	W	S	P	C	U	Y	T	J	A	F	H	R	D	I	Z	O	N	V	X
k	P	U	Y	R	N	E	L	C	D	F	A	M	T	Q	G	I	H	J	V	O	Z	K	B	X	S	W
l	T	C	V	M	H	G	Q	D	O	N	U	X	E	R	W	P	B	A	L	I	S	F	J	K	Y	Z
m	M	T	N	Z	J	K	A	L	F	G	P	H	S	I	X	R	Y	W	U	C	V	E	D	O	Q	B
n	O	V	X	N	M	D	I	E	T	U	K	Q	W	Y	P	S	R	C	J	B	A	G	H	F	Z	L
o	L	S	T	H	I	C	W	Y	R	V	E	Z	D	J	K	X	U	N	P	G	M	Q	F	B	A	O
p	Z	R	A	E	B	V	S	X	K	I	Q	L	U	N	D	Y	W	G	O	F	P	T	C	H	J	M
q	B	X	C	K	L	Y	R	N	P	S	F	I	Z	H	T	O	M	V	W	U	E	D	Q	A	G	J
r	S	Y	H	I	X	W	J	O	B	M	G	D	V	K	Z	E	P	L	C	R	T	U	A	Q	N	F
s	E	D	F	V	Q	P	N	G	Z	A	B	W	O	U	I	J	T	R	Y	H	X	M	L	S	K	C
t	K	Z	G	X	Y	M	E	J	I	L	V	F	H	P	C	T	A	S	Q	N	O	W	U	D	B	R
u	R	Q	M	D	C	I	B	P	V	W	H	S	F	L	N	Z	J	T	X	A	U	O	G	Y	E	K
v	D	F	J	T	U	L	G	I	M	C	N	P	Q	V	A	K	O	B	H	Z	W	S	X	E	R	Y
w	U	P	O	B	Z	Q	V	H	C	K	R	Y	M	W	S	G	D	E	A	X	J	L	T	I	F	N
x	V	W	L	P	S	J	F	T	X	H	Y	A	K	D	E	N	I	O	G	M	R	B	Z	U	C	Q
y	F	A	U	J	W	N	O	M	E	T	I	K	X	B	L	C	Q	Z	S	P	D	Y	R	V	H	G
z	I	N	W	G	V	R	C	Q	Y	O	J	T	A	M	U	H	S	F	B	K	L	P	E	Z	X	D

Slide 10

Addition and multuplication

The Vigenère square is a Latin square with a particularly simple structure: each row shifts along one place, and the last entry comes back to the start. This can be explained another way, using *modular arithmetic*. If, instead of the letters `A,...,Z`, we use the numbers $0, \dots, 25$, then the entry in row i and column j of the square is $i + j$, where the addition is mod 26: that is, instead of saying $11 + 18 = 29$, we put $11 + 18 = 3$. (That is, if the sum is 26 or more, we subtract 26 from the answer; in other words, we take the remainder on dividing by 26.)

The same construction works with any number n in place of 26, and always gives us a Latin square with the same structure.

What happens if we use multiplication mod n rather than addition?

Slide 11

Examples: integers mod 5 and 6

$n = 5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$n = 6$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Slide 12

Rings and fields

Since $0 \times x = 0$ for all x, we have to leave out the row and column zero. We see that, for $n = 5$, the other rows do give us a Latin square; for $n = 6$ they don't (we get 0 appearing in other rows, and we get elements like $2, 3, 4$ repeated).

A system where we can add, subtract, and multiply is called a *ring*. Thus, the integers mod n form a ring. The addition table of a ring is always a Latin square.

If we can also divide, then the system is called a *field*. It is known that the integers mod n form a field if and only if n is a prime number.

Slide 13

Experimental design

Suppose that we have to test nine different types of pesticides on apple trees. We have an orchard with 81 trees planted in a square grid.

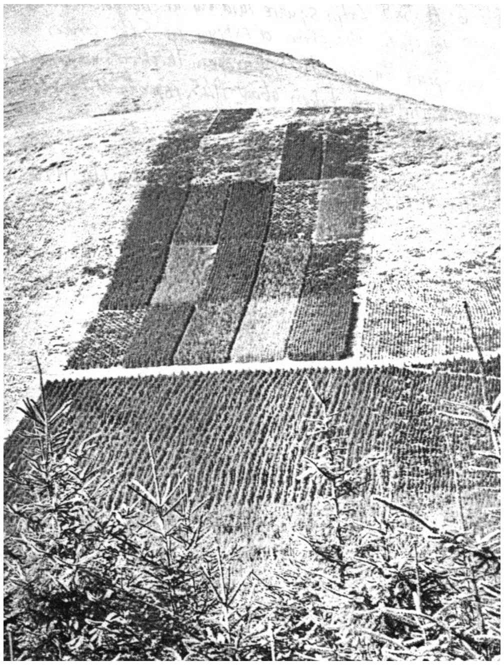
We could just put pesticide 1 on the trees in the first row, 2 on the second row, etc. But, unknown to us, the orchard is on a hillside, and trees lower down the slope tend to produce more apples; so we couldn't tell whether the experimental results show a difference in the pesticides or just the difference caused by the slope.

Similarly, we could put pesticide 1 on the first column, and so on; but there is a road on one side of the orchard and a stream on the other, and these could also affect production.

In these circumstances we should use a Latin square. This will ensure that the nine pesticides are equally affected by differences in height and in distance from the road or the stream.

The next slide shows an experiment on trees designed using a Latin square.

Slide 14



An experiment in Bettgelert Forest, Wales, designed by R. A. Fisher.

Slide 15

Su Doku in experimental design

The easiest Latin square is the addition table of integers mod 9: label the rows, columns and pesticides by $0, \ldots, 8$ and put pesticide $i + j$ on the tree on row i and column j. But, unknown to us, there is a fertile patch in the middle of the field (in rows and columns $3, 4, 5$). Thus pesticide 8 would go on three trees in the fertile spot, 7 and 0 on two, 6 and 1 on just one, and the others would not occur at all.

If instead we use the solution to a Su Doku, we fix this problem too, since every pesticide will be used on just one tree in the fertile patch. The extra constraint "mixes" the numbers up better.

Slide 16

Solving a Su Doku

Let us come back to the question: How do you solve a Su Doku?

Look back at the original puzzle. We'll take a look at the 3×3 square in the bottom left of the puzzle, and number its cells (i, j), where i and j take the values $1, 2, 3$. The five blank squares are $(1, 1)$, $(1, 2)$, $(1, 3)$, $(2, 1)$ and $(3, 3)$.

Cell $(1, 1)$ has 8 and 7 in the same row, 1 and 2 in the same column, and $1, 2, 3, 5$ in the same subsquare. So the number we put there must be one of $4, 6, 9$. Similarly we find the possibilities for $(1, 2)$ are $4, 6, 9$, for $(1, 3)$ also $4, 6, 9$), for $(2, 1)$ are $4, 6, 7, 8, 9$, and for $(3, 3)$ are $4, 6, 7, 9$.

Slide 17

Hall's Theorem

Suppose you have to arrange marriages between n boys and n girls. You can only marry a boy and girl if they already know each other. Is it possible to arrange all the marriages?

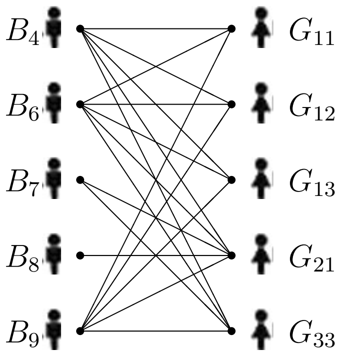
If the marriages can be arranged, then any group of k girls must between them know at least k boys. The mathematician Philip Hall proved that this *necessary* condition is also *sufficient*: that is, if every set of girls satisfies this condition, then the marriages can be arranged. This is *Hall's marriage theorem.*

A set of k girls who between them know exactly k boys is called a *critical set.* If a critical set exists, then these girls must be married off to the boys they know, who are then unavailable for marrying other girls, and can be deleted from their lists.

Slide 18

An example

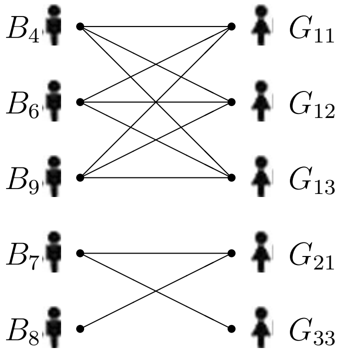
We encode the subsquare of the Su Doku puzzle as a marriage problem. Here the boys are the available numbers, and the girls are the empty cells. Placing a number in each cell is equivalent to marrying off all the girls.



Slide 19

First reduction

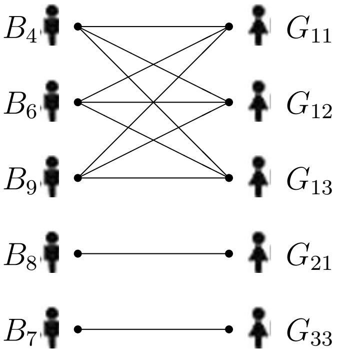
We see that the set G_{11}, G_{12}, G_{13} is critical: these three girls between them know only boys B_4, B_6, B_9. So we can remove these boys from the acquantances of the other two girls.



Slide 20

Second reduction

Now G_{33} is critical since she knows only B_7, so we can delete B_7 from G_{12}'s options.



Now we see that B_7 must marry G_{33} and B_8 must marry G_{21}. So we can put the entry 7 in box $(3, 3)$ and the entry 8 in box $(2, 1)$ in the puzzle.

Continue in this way until the solution is found.

Disclaimer: This method does not solve every Su Doku puzzle: the mathematician Gordon Royle has found examples where it fails. But it works on every example I have tried from the newspapers.