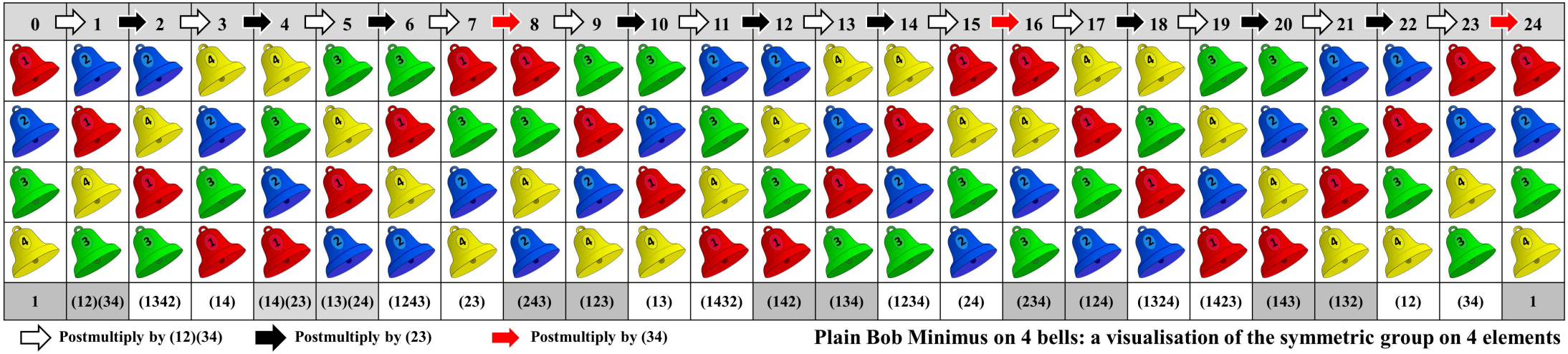
THEOREM OF THE DAY

Sylow's Theorems *Let G be a finite group of order $p^n m$ where p is a prime not dividing m. Then*

1. *G has subgroups of order p^n. Any subgroup of this order, termed a p-Sylow subgroup, is conjugate to any other;*
2. *any subgroup of G of p-power order is contained in a p-Sylow subgroup;*
3. *the number of p-Sylow subgroups divides m, and is 1 more than a multiple of p.*



Plain Bob Minimus on 4 bells: a visualisation of the symmetric group on 4 elements

Lagrange's Theorem says that a finite group can only have subgroups whose orders divide its own order. It is natural to ask if this division property guarantees the existence of a subgroup. We have such a guarantee if the dividing number is a prime: this is Cauchy's Theorem; but it does not generalise to arbitrary subgroup orders. Consider our illustration of the symmetric group Sym_4 of all 24 permutations of four objects. It happens that every number dividing 24 is the order of a subgroup of Sym_4. But the subgroup of order 12, which comprises the permutations shaded in the bottom row of our table, does not itself have a subgroup of order 6. Instead, the subgroups of Sym_4 of order 6 consist of permutations which lie partly inside the shaded subgroup and partly outside it.

Indeed, the subgroups of Sym_4 of order 6 are precisely Sym_3, being permutations numbers 0, 7, 9, 10, 21 and 22, and its *conjugates*. Conjugating a permutation p by another, q, means applying q to the entries of p. For example, conjugating (123) by (12)(34) gives (214), which is the same cycle as (142). (More generally, conjugation of p by q in an arbitrary group is defined as the product $q^{-1}pq$). The conjugate of Sym_3 by (12)(34) in Sym_4 can be calculated to be the subgroup consisting of permutations numbers 0, 3, 12, 15, 17, and 22.

Sylow's theorems tell us, and very explicitly, how Cauchy's theorem extends from primes to prime powers. For our example, we have $24 = 2^3 \times 3^1$. So there are 2-Sylow subgroups of order 8: the permutations defining the bell-ringing method above start with just such a subgroup, comprising permutations 0 to 7. Conjugating this subgroup by, for instance, (12), produces a second 2-Sylow subgroup; conjugating by (13) gives a third. And Sylow's 3rd theorem (part 3 above) tells us there are no more. There are eight permutations lying in none of the 2-Sylow subgroups: these are the 3-cycles. Together with the identity permutation (permutation 0) they form four 3-Sylow subgroups. Again by 'Sylow-3' there are no more (8 would divide m but is 2 more than a multiple of 3).

Ludwig Sylow (pronounced, for anglophones, roughly as in '**Seal of** approval') discovered his three theorems around 1870 through his study of Galois' work from the 1820s, rather than as a deliberate extension of Cauchy's 1845 theorem.

Web link: kconrad.math.uconn.edu/blurbs/

Further reading: Topics in Group Theory by Geoff Smith and Olga Tabachnikova, Springer, 2000.