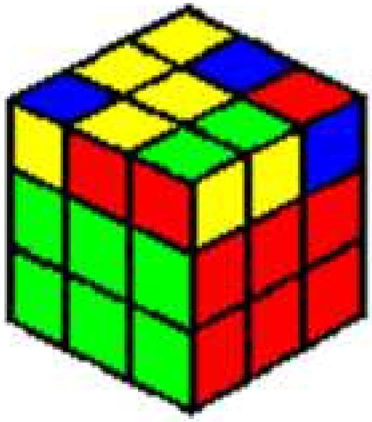
THEOREM OF THE DAY

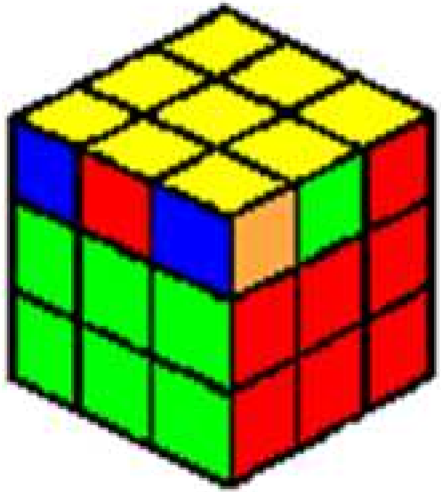
Theorem (Fermat's Little Theorem) *If p is a prime number, then*

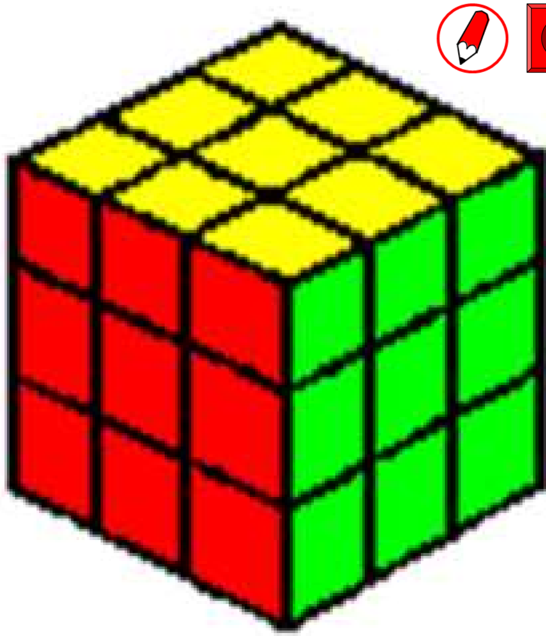
$$a^{p-1} \equiv 1 \pmod{p}.$$

for any positive integer a not divisible by p.

Proof:
If all factors are taken modulo p then the product $a \times 2a \times \ldots \times (p-1)a$ is identical to $1 \times 2 \times \ldots \times (p-1)$ because if $ka = k'a \pmod{p}$, for some multiples $k < k' < p$, then p divides $a(k'-k)$ and therefore divides one of a and $(k'-k)$. But p does not divide a, by hypothesis and $k'-k < p$. Therefore $a^{p-1} \times (p-1)! = (p-1)! \pmod{p}$ so $a^{p-1} = 1 \pmod{p}$.







Suppose $p = 5$. We can imagine a row of a copies of an $a \times a \times a$ Rubik's cube (let us suppose, although this is not how Rubik created his cube, that each is made up of a^3 little solid cubes, so that is a^4 little cubes in all.) Take the little cubes 5 at a time. For three standard 3×3 cubes, shown here, we will eventually be left with precisely one little cube remaining. Exactly the same will be true for a pair of 2×2 'pocket cubes' or four of the 4×4 'Rubik's revenge' cubes. The 'Professor's cube', having $a = 5$, fails the hypothesis of the theorem and gives remainder zero.

The converse of this theorem, that $a^{p-1} \equiv 1 \pmod{p}$, for some a not dividing p, implies that p is prime, does not hold. For example, it can be verified that $2^{340} \equiv 1 \pmod{341}$, while 341 is not prime. However, a more elaborate test *is* conjectured to work both ways: remainders add, so the Little Theorem tells us that, modulo p, $1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv \overbrace{1 + 1 + \ldots + 1}^{p-1} = p - 1$. The 1950 conjecture of the Italian mathematician Giuseppe Giuga proposes that this *only* happens for prime numbers: a positive integer n is a prime number if and only if $1^{n-1} + 2^{n-1} + \ldots + (n-1)^{n-1} \equiv n - 1 \pmod{n}$. Jonathan Borwein has shown that any counterexample must have over 4771 prime factors and over 19908 digits!

Fermat announced this result in 1640, in a letter to a fellow civil servant Frénicle de Bessy. As with his 'Last Theorem' he claimed that he had a proof but that it was too long to supply. In this case, however, the challenge was more tractable: Leonhard Euler supplied a proof almost 100 years later which, as a matter of fact, echoed one in an unpublished manuscript of Gottfried Wilhelm von Leibniz, dating from around 1680.

Web link: artofproblemsolving.com/wiki/index.php?title=Fermat's_Little_Theorem. The cube images are from: www.ws.binghamton.edu/fridrich/.

Further reading: *Elementary Number Theory, 6th revised ed.,* by David M. Burton, MacGraw-Hill, 2005, chapter 5.