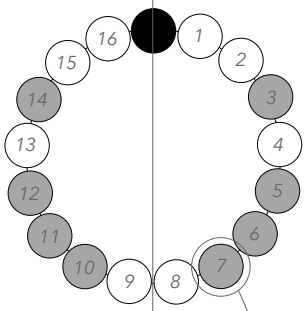
Development of Fermat's Little Theorem

Robert Atkinson
November 2021

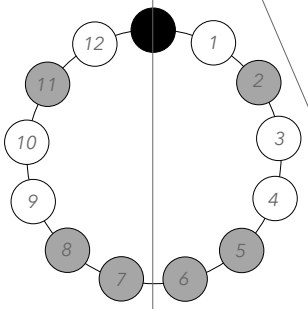
modulo 17

power 8



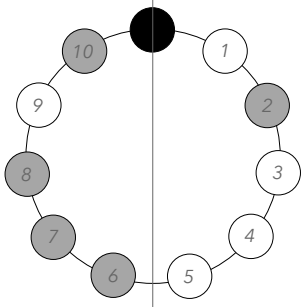
modulo 13

power 6



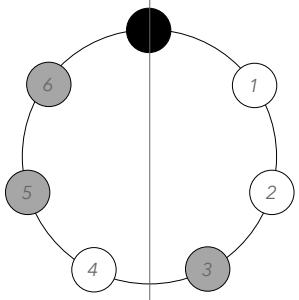
modulo 11

power 5



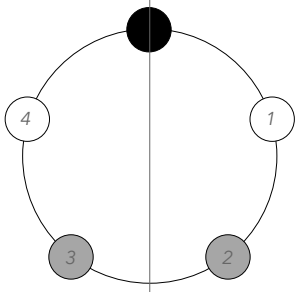
modulo 7

power 3



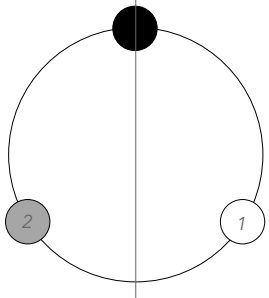
modulo 5

power 2



modulo 3

power 1



By Fermat's Little Theorem:

If $a \not\equiv 0 \pmod{p}$ and p is prime

then $a^{(p-1)} \equiv 1 \pmod{p}$

Development of Fermat's theorem:

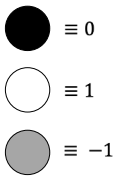
1. For any x modulo p, if $x^2 \equiv 1$, then $x \equiv 1 \text{ or } -1 \pmod{p}$
2. Let $x^2 = a^{(p-1)}$
3. Because p is a prime number, $p-1$ is always even (other than when $p = 2$), so $\left(\frac{p-1}{2}\right)$ is always an integer. An integer raised to the power $\left(\frac{p-1}{2}\right)$ is also an integer, and can be used in a modulus calculation
4. From (2) and (3), $x = a^{\left(\frac{p-1}{2}\right)}$, so from (1), $a^{\left(\frac{p-1}{2}\right)} \equiv 1 \text{ or } -1 \pmod{p}$

Conclusion:

If $a \not\equiv 0 \pmod{p}$ and p is prime

then $a^{\left(\frac{p-1}{2}\right)} \equiv 1 \text{ or } -1 \pmod{p}$

The conclusion is confirmed by the test results shown on the left, which also show the arrangement of 1 and -1 congruences. The diagrams show modulus rings for prime-numbered moduli (p) from 3 to 17, showing 1 or -1 congruences when each modulus element (a) is raised to the power $a^{\left(\frac{p-1}{2}\right)}$



An application:

Find the least residue of 7^24 (mod 17).
This would be difficult using Fermat's theorem, which would only help if the power was (or was close to) 16 or a multiple. The power of 24 is, however, a multiple of 8, so the result can be seen to be (from the diagram) ≡ -1^3 ≡ -1 ≡ 16 (mod 17).

Further observations:

1. The number of congruent 1 and congruent -1 elements is the same within each example, and equals the power of a.

2. The congruencies therefore sum to 0, unlike Fermat's theorem, where they sum to p-1.

*3. The congruent 1 and -1 elements are arranged symmetrically around the vertical axis of the modulus ring. (see * below)*

4. The symmetry is positive (same elements) where the power is even; negative (opposite elements) where the power is odd.

5. If the power is even, then the congruent 1 elements further 'decompose' into a mixture of congruent 1 and congruent -1 elements when the power is again halved.

** Modulus elements appear always to be arranged symmetrically within an odd-numbered modulus for any power, when the residues are expressed as -(p-1)/2, ... -2, -1, 0, 1, 2, ... (p-1)/2*