Builtins List

The following table lists the different builtins implemented
in the Cairo VM and gives a brief description of their purpose.
For each builtin, a specific section details how it works,
its cells organization if any, and references their actual
implementation in different implementations of the Cairo VM.
Additional resources related to the operation performed
by the builtin are provided if relevant.

Builtin	Description
[Output][output]	Stores all the public memory needed to generate a STARK proof (input & output values, builtin pointers...)
[Pedersen][pedersen]	Computes the Pedersen hash `h` of two felts `a` and `b`. `h = Pedersen(a, b)`
[Range Check][rc]	Verify that a felt `x` is within the bounds `[0, 2**128)`.
[ECDSA][ecdsa]	Verify that the ECDSA signature of a given public key `pub` on a message `m` equals `sig`, previously stored. Only used by Cairo Zero.
[Bitwise][bitwise]	Computes the bitwise AND, XOR and OR of two felts `a` and `b`. `a & b`, `a ^ b` and `a | b`.
[EC OP][ec_op]	Performs Elliptic Curve OPerations - For two points on the STARK curve `P`, `Q` and a scalar `m`, computes `R = P + mQ`.
[Keccak][keccak]	Computes the new state `s'` after applying the 24 rounds of the keccak-f1600 block permutation on a given state `s`.
[Poseidon][poseidon]	Computes the new state `s'` after applying the 91 rounds of the hades block permutation on a given state `s`.
[Range Check96][rc96]	Verify that a felt `x` is within the bounds `[0, 2**96)`.
[AddMod][add_mod]	Arithmetic Circuit Support - Computes the modular addition `c` of two felts `a`, `b` by batches. `c "a a + b mod(p)`
[MulMod][mul_mod]	Arithmetic Circuit Support - Computes the modular multiplication `c` of two felts `a`, `b` by batches. `c "a a * b mod(p)`
[Segment Arena][seg_are]	Manages the Cairo dictionaries Not used in Cairo Zero.
[Gas][gas]	Manages the available gas during the run. Used by Starknet to handle its gas usage and avoid DoS.
[System][system]	Manages the Starknet syscalls & cheatcodes.

[output]: ch204-02-00-output.md
[pedersen]: ch204-02-01-pedersen.md
[rc]: ch204-02-02-range-check.md
[ecdsa]: ch204-02-03-ecdsa.md
[bitwise]: ch204-02-04-bitwise.md
[ec_op]: ch204-02-05-ec-op.md

[keccak]: ch204-02-06-keccak.md
[poseidon]: ch204-02-07-poseidon.md
[rc96]: ch204-02-08-range-check-96.md
[add_mod]: ch204-02-09-add-mod.md
[mul_mod]: ch204-02-10-mul-mod.md
[seg_are]: ch204-02-11-segment-arena.md
[gas]: ch204-02-12-gas.md
[system]: ch204-02-13-system.md