fn floor_div

Michael Shoemate

This proof resides in **"contrib"** because it has not completed the vetting process.

Proves soundness of the implementation of `floor_div` in `mod.rs` at commit f5bb719 (outdated[1]).

1 Hoare Triple

Precondition

Compiler-Verified

None

User-Verified

None

Pseudocode

In the following pseudocode, define / as zero integer division, as used by the Rust Dashu dependency's IBig. Zero integer division is real division that is then rounded towards zero. This differs from Python's division, which converts to float, and Python's integer division, which is the desired floor integer division.

```
def floor_div(a: IBig, b: UBig) -> IBig:
    if Sign.Positive == a.sign():
        return a / b
    else:
        return (a - b + 1) / b
```

Postcondition

Theorem 1.1. Return $floor(a/b)$, where / denotes real division.

Proof. Consider the following cases:

- If $a \geq 0$ then zero integer division and floor integer division are equivalent. Therefore the result is $floor(a/b)$.
- If $a < 0$ then $b-1$ is subtracted before zero integer division. This shifts the problematic upper elements that would round up into the range that rounds down, while the lower elements that would round down now round up, resulting in the correct floor division. Therefore the result is $floor(a/b)$.

In all cases, the result is $floor(a/b)$. □

[1] See new changes with `git diff f5bb719..699e261 rust/src/measurements/noise/nature/float/utilities/mod.rs`