compArith notes

- $\mathbb{B}$ is defined as a finite set with two elements `Fin 2`.
- Simplified the def of $[\![-]\!]$ to just $\Sigma_{i=0}^{i=k} x_i * 2^i$, which is implemented for vectors as:

$$
\begin{aligned}
\Sigma\ [\,] &= 0 \\
\Sigma\ (0 :: xs^k) &= \Sigma\ xs^k \\
\Sigma\ (1 :: xs^k) &= 2^k + \Sigma\ xs^k
\end{aligned}
$$

  where x^k is a vector of booleans of size k (`Vec 𝔹 k` in agda).
- Use $\langle\langle - \rangle\rangle$ instead of $(\!|-|\!)$ because agda does not support such symbol
- Defined $MOD\ 2$ as `_mod𝔹`:

$$
\begin{aligned}
0\ \texttt{mod}\mathbb{B} &= 0 \\
suc\ 0\ \texttt{mod}\mathbb{B} &= 1 \\
suc\ (suc\ a)\ \texttt{mod}\mathbb{B} &= a
\end{aligned}
$$

- Defined $DIV\ 2$ as `_div𝔹`:

$$
\begin{aligned}
0\ \texttt{div}\mathbb{B} &= 0 \\
suc\ 0\ \texttt{div}\mathbb{B} &= 0 \\
suc\ (suc\ a)\ \texttt{mod}\mathbb{B} &= 1
\end{aligned}
$$

  Since we only ever do $(a+b+c) DIV\ 2$ where $a, b, c \in \mathbb{B}$, we can show that $(a+b+c)\ \texttt{div}\mathbb{B} \equiv (a+b+c)\ DIV\ 2$ (lemma `div𝔹spec`)
- Defined bitwise addition of two vectors a, b of the same length k as a tuple (rs, c), where rs is the resulting vector of length k and c is the *carry* c_{k+1}.

$$
\begin{aligned}
[\,] \oplus [\,] &= ([\,],\ 0) \\
(a :: as) \oplus (b :: bs) &= (r :: \mathsf{fst}\ (as \oplus bs), c) \\
&\text{where} \\
&\qquad r = (a + b + \mathsf{snd}\ (as \oplus bs))\ \texttt{mod}\mathbb{B} \\
&\qquad c = (a + b + \mathsf{snd}\ (as \oplus bs))\ \texttt{div}\mathbb{B}
\end{aligned}
$$