Chapter 5

Reserves Recitation.

5.1

Another sorting algorithms, that it's correctness isn't so obivoius.

```
Result: returns the multiplication $x \cdot y$ where $x, y \in \mathbb{F}_2^n$
for $i \in [n]$ do
    for $j \in [n]$ do
        if $A_j < A_i$ then
            swap $A_i \leftrightarrow A_j$
        end
    end
end
```

```
Result: returns the multiplication $x \cdot y$ where $x, y \in \mathbb{F}_2^n$

if $x, y \in \mathbb{F}_2$ then
    return $x \cdot y$
end

else
    define $x_l, x_r \leftarrow x$ and $y_l, y_r \leftarrow x$      // $O(n)$.

    calculate $z_0 \leftarrow$ Karatsuba $(x_l, y_l)$
              $z_2 \leftarrow$ Karatsuba $(x_r, y_r)$
              $z_1 \leftarrow$ Karatsuba $(x_r + x_l, y_l + y_r) - z_0 - z_2$

    return $z_0 + 2^{\frac{n}{2}} z_1 + 2^n z_2$      // $O(n)$.
end
```