T-79.4501 Cryptography and Data Security **Spring 2006**

Here is a small example to illustrate division of polynomials for homework 2, excercise 1b. The task was to use Extended Euclidean algorithm to compute inverse of $x^3 + x \mod x^5 + x^2 + x^1$.

Now, the setup is $r_0 = x^5 + x^2 + 1$ and $r_1 = x^3 + x$, and first we are trying to solve q_2 and r_2, so that $r_0 = q_2 \cdot r_1 + r_2$.

$$
\begin{array}{r|r}
 & x^2 \qquad\qquad + 1 \\ \hline
x^3 + x & x^5 + 0x^4 + 0x^3 + x^2 + 0x + 1 \\
 & x^5 + \qquad x^3 \qquad\qquad\qquad \\ \cline{2-2}
 & x^3 + x^2 + 0x + 1 \\
 & x^3 + \qquad x \qquad \\ \cline{2-2}
 & x^2 + x + 1
\end{array}
$$

As calculations are performed $\mod 2$, there is no need to separate addition and subtraction.

So, we get $q_2 = x^2 + 1$ and $r_2 = x^2 + x + 1$. This can be verified:
$(x^2+1)\cdot(x^3+x)+(x^2+x+1) = (x^5+x^3+x^3+x)+(x^2+x+1) \equiv x^5+x^2+1$.