Last time: polynomial addition, subtraction, multiplication and division in $\mathbb{Z}_3[x]$, $\mathbb{Z}_5[x]$, $\mathbb{Z}_7[x]$, $\mathbb{Z}_{11}[x]$, ...

Example Let's divide $2x^2+3x+4$ into x^4+2x+2 working over $\mathbb{Z}_7$.

$$
\begin{array}{r}
4x^2 + x + 1 \\
2x^2+3x+4 \overline{)\, x^4+2x+2} \\
x^4+5x^3+2x^2 \\
\hline
-5x^3-2x^2+2x+2 \\
2x^3+3x^2+4x \\
\hline
-5x^2-2x+2 \\
2x^2+3x+4 \\
\hline
-5x-2
\end{array}
$$

So

$$x^4+2x+2 = (4x^2+x+1)(2x^2+3x+4) + (2x+5)$$

in $\mathbb{Z}_7[x]$.

Example Let's consider

$$f(x) = x^3 + 3x^2 + 3x + 2$$

in $\mathbb{Z}_7[x]$. Can we factorize $f(x)$?

$f(0) \equiv 2 \mod 7$

$f(1) \equiv 2 \mod 7$

$f(2) \equiv 1 + 5 + 6 + 2 \equiv 0 \mod 7$

If we use our algorithm to divide $(x-2)$ into $f(x)$ we'd get

$$f(x) = q(x)(x-2) + r(x)$$

with degree of $r(x)$ less than 1.

So $r(x) = r \in \mathbb{Z}_7$.

Thus

$$f(x) = q(x)(x-2) + r.$$

But

$0 = f(2) = q(x) \cdot 0 + r$, and $r = 0$.

Hence $(x-2)$ divides $f(x)$.

Let's continue

$f(x) = x^3 + 3x^2 + 3x + 2$

$f(3) \equiv -1 - 1 + 2 + 2 = 2.$

$f(4) \equiv 1 - 1 + 5 + 2 \not\equiv 0$

$f(5) \equiv -1 + 5 + 1 + 2$

$f(6) \not\equiv 0 \mod 7$

Hence $x-2$ is the only factor of degree 1.

Thus

$$(x^3 + 3x^2 + 3x + 2) = (x-2)(x^2 + 5x + 6)$$

$$\begin{array}{r} x^2 + 5x + 6 \\ x-2 \overline{)\, x^3 + 3x^2 + 3x + 2} \\ \underline{x^3 - 2x^2} \\ 5x^2 + 3x + 2 \\ \underline{5x^2 - 3x} \\ 6x + 2 \\ \underline{6x + 2} \\ 0 \end{array}$$

Note : x^2+5x+6 is

irreducible since, $g(x)=x^2+5x+6$

satisfies

$g(0) \not\equiv 0 \mod 7$

$g(1) \not\equiv 0$

$g(2) \not\equiv 0$

$g(3) \not\equiv 0$

$g(4) \not\equiv 0$

$g(5) \not\equiv 0$

$g(6) \not\equiv 0$.

Example Let factorize

$f(x) = x^3+3x^2+3x+2$

in $\mathbb{Z}_5[x]$.

$f(0) \equiv 2 \mod 5$

$f(1) \equiv 4 \mod 5$

$f(2) \equiv 3+2+1+2 = 3 \mod 5$

$f(3) \equiv 2+2+4+2 \equiv 0$

$f(4) \equiv -1+3-3+2 \not\equiv 0$.

So $(x-3)$ is the only factor of degree 1.

observation: factorization in $\mathbb{Z}_p[x]$ depends very much on the prime p.

Remark Such calculations, factorizations etc. are fine in $\mathbb{Z}_p[x]$ for any prime p. But they won't always work when p is not prime.

Example Let's try to divide $2x^2+3x+4$ into x^4+2x+2 in $\mathbb{Z}_4[x]$.

$2x^2+3x+4 \overline{)\, x^4+2x+2}$

$2 \times 0 \equiv 0 \mod 4$

$2 \times 1 \equiv 2 \mod 4$

$2 \times 2 \equiv 0 \mod 4$

$2 \times 3 \equiv 2 \mod 4$

2^{-1} does not exist mod 4, so the division algorithm breaks down.