Discuss in your group: Given this Mathematica output

You can ignore this.

```
In[3]:= f = 4 x^5 + 2 x^3 + 4 x + 1

In[4]:= PolynomialQuotientRemainder[f, x^2 - 1, x]

Out[4]= {4 x^3 + 6 x, 10 x + 1}
```

d(x)

q(x) r(x)

describe how $f(x)$, $x^2 - 1$, $4x^3 + 6x$, and $10x + 1$ are related.

Answer: $f(x) = (x^2 - 1) \cdot (4x^3 + 6x) + (10x + 1)$.

$$d(x) \quad \cdot \quad q(x) \quad + \quad r(x)$$

Key: $\deg r(x) < \deg d(x)$, i.e., the remainder is "less" than the divisor.

Consider the polynomial ring $\mathbb{Z}_7[x]$ and a subset

$$\langle x^2 - 1 \rangle = \{(x^2 - 1) \cdot q(x) \mid q(x) \in \mathbb{Z}_7[x]\},$$

i.e., the principal ideal generated by $x^2 - 1$ (or the set of all multiples of $x^2 - 1$).

The quotient ring $\mathbb{Z}_7[x]/\langle x^2 - 1 \rangle$ contains cosets of the form

$$a(x) + \langle x^2 - 1 \rangle \quad \text{where } a(x) \in \mathbb{Z}_7[x].$$

Note: This is just like $\mathbb{Z}/5\mathbb{Z}$, which contains the cosets $a + 5\mathbb{Z}$.

Problem #2: Let $f(x) = 4x^5 + 2x^3 + 4x + 1 \in \mathbb{Z}_7[x]$ and recall that

$$f(x) = (x^2 - 1) \cdot (4x^3 + 6x) + (3x + 1).$$

- $f(x) \neq 3x + 1$ in $\mathbb{Z}_7[x]$, they're *different* polynomials.

- But in $\mathbb{Z}_7[x]/\langle x^2 - 1\rangle$, their cosets are the *same*, i.e.,

$$f(x) + \langle x^2 - 1\rangle = (3x + 1) + \langle x^2 - 1\rangle, \quad \longleftarrow \text{“reduce”} \ f(x) + \langle x^2 - 1\rangle.$$

because $f(x) - (3x + 1) = (x^2 - 1) \cdot (4x^3 + 6x) \in \langle x^2 - 1\rangle$.

Key: Compare this with how $378 \neq 3$ in $\mathbb{Z}$,

but $378 + 5\mathbb{Z} = 3 + 5\mathbb{Z}$ in $\mathbb{Z}/5\mathbb{Z}$, because $378 - 3 \in 5\mathbb{Z}$.

Problem #5: We have $x^2 + \langle x^2 - 1 \rangle = 1 + \langle x^2 - 1 \rangle$, since $x^2 - 1 \in \langle x^2 - 1 \rangle$.

Let $f(x) = 4x^5 + 2x^3 + 4x + 1 \in \mathbb{Z}_7[x]$ again. Then...

$$f(x) + \langle x^2 - 1 \rangle = (4x^5 + 2x^3 + 4x + 1) + \langle x^2 - 1 \rangle$$

$$= (4 \cdot x^2 \cdot x^2 \cdot x + 2 \cdot x^2 \cdot x + 4x + 1) + \langle x^2 - 1 \rangle$$

$$= (4 \cdot 1 \cdot 1 \cdot x + 2 \cdot 1 \cdot x + 4x + 1) + \langle x^2 - 1 \rangle$$

$$= (3x + 1) + \langle x^2 - 1 \rangle$$

Key: Treat x^2 and 1 to be the same *as coset representatives.*

But $x^2 \neq 1$ in $\mathbb{Z}_7[x]$ as polynomials.

Zero divisors in $\mathbb{Z}_7[x]/\langle x^2 - 1\rangle$

$$((x+1) + \langle x^2 - 1\rangle) \cdot ((x-1) + \langle x^2 - 1\rangle) = (x+1)(x-1) + \langle x^2-1\rangle$$

$$= (x^2-1) + \langle x^2-1\rangle$$

$$= 0 + \langle x^2-1\rangle$$

each factor $\neq 0 + \langle x^2 - 1\rangle$

$\Longrightarrow$ $(x+1) + \langle x^2 - 1\rangle$ and $(x-1) + \langle x^2 - 1\rangle$ are zero divisors, hence *not* units.

$\Longrightarrow$ $\mathbb{Z}_7[x]/\langle x^2 - 1\rangle$ is *not* a field.

Theorem: Let F be a field and fix $g(x) \in F[x]$.

If $g(x)$ is factorable, then $F[x]/\langle g(x) \rangle$ is *not* a field.

Example:

$\mathbb{Z}_7[x]/\langle x^2 - 1 \rangle$.

Proof: Assume that $g(x)$ is factorable.

Then $g(x) = p(x) \cdot q(x)$ where $p(x),\, q(x) \in F[x]$, with $\deg p(x),\, \deg q(x) < \deg g(x)$.

We have...

$$\begin{aligned}(p(x) + \langle g(x) \rangle) \cdot (q(x) + \langle g(x) \rangle) &= p(x) \cdot q(x) + \langle g(x) \rangle \\ &= g(x) + \langle g(x) \rangle \\ &= 0 + \langle g(x) \rangle\end{aligned}$$

$\neq 0 + \langle x^2 - 1 \rangle$

Since $\deg p(x),\, \deg q(x) < \deg g(x)$, neither $p(x)$ nor $q(x)$ is a multiple of $g(x)$.

Thus, neither $p(x) + \langle g(x) \rangle$ nor $q(x) + \langle g(x) \rangle$ is equal to $0 + \langle g(x) \rangle$.

Hence, they are zero divisors in $F[x]/\langle g(x) \rangle$, so that they are *not* units.

Thus, $F[x]/\langle g(x) \rangle$ is *not* a field.