MATHEMATICAL ENRICHMENT   JAN 29th, 2022

Kevin Hutchinson: Algebra

Is $1572^2 - 471^2$ prime?

$$\shortparallel$$

No: $(1572 + 471) \cdot (1572 - 471)$.

Universal law of algebra:

$$x^2 - y^2 = (x-y)(x+y)$$

"**Polynomials**" (in 2 variables)

$$\ldots + \underset{\text{coefficient}}{11}\, \underbrace{x^5 y^7}_{\substack{\text{degree} \\ 12.}} + \cdots$$

$$x^3 - y^3 \underset{\text{factor} \to}{=} (x-y)(x^2 + xy + y^2)$$

Check. RHS $= x^3 + \cancel{x^2 y} + \cancel{x y^2}$
$\qquad - \cancel{x^2 y} - \cancel{x y^2} - y^3$

In general we have

$$x^n - y^n = (x-y)\underbrace{(x^{n-1} + x^{n-2} y + \ldots + x^{n-k} y^{k-1} + \ldots + x y^{n-2} + y^{n-1})}_{\text{homogeneous of degree } n-1}$$

degree $n-1$

$x^3 y^2 + x^5 y^7$ ← not homogeneous.

$n=4$: $x^4 - y^4 = (x-y)\underbrace{(x^3 + x^2y + xy^2 + y^3)}_{\substack{\shortparallel \\ (x+y)(x^2+y^2)\ \checkmark}}$

$$= (x-y)(x+y)(x^2+y^2)$$

Or else:

$$\left[\ x^4 - y^4 = (x^2)^2 - (y^2)^2 = (x^2 - y^2)(x^2+y^2) \right.$$
$$\left. = (x-y)(x+y)(x^2+y^2)\ \right]$$

Does x^2+y^2 factor further?

$$\left(\ (x+y)^2 = x^2 + y^2 + 2xy\ \right)$$

The answer depends on the rules of the game: i.e. what kinds of coefficients do we allow.

Let's allow complex numbers: $a + bi$

$$i = \sqrt{-1} \ :\ \text{ie}\ \ i^2 = -1$$

$$(a+bi)(c+di) = (ac - bd) + i(bc + ad)$$

$$(5+2i)(3-4i) = (15+8) + i(6-20)$$
$$= 23 - 14i$$

linear polynomials

Then $x^2 + y^2 = x^2 - (iy)^2 = (x - iy)(x+iy)$

We say that x^2+y^2 factors over $\mathbb{C}$

Complex numbers.

Exercise x^2+y^2 does not factor over $\mathbb{R}$

Factor x^4+y^4 as a product of two degree 2 polynomials <u>over</u> $\mathbb{R}$.

$$x^4+y^4 = \underbrace{x^4+2x^2y^2+y^4}\ \underbrace{-2x^2y^2}$$

$$= (x^2+y^2)^2-(\sqrt{2}xy)^2$$

$$= (x^2+y^2+\sqrt{2}\,xy)(x^2+y^2-\sqrt{2}\,xy)$$

real, but <u>not</u> rational.

rational := $\frac{\text{integer}}{\text{integer}}$. $\sqrt{2} \neq \frac{\text{integer}}{\text{integer}}$ ..

$\mathbb{Q}$ = set of all rational numbers.

x^4+y^4 factors <u>over</u> $\mathbb{R}$.

(It factors further over $\mathbb{C}$)

x^4+y^4 does not factor over $\mathbb{Q}$. It is <u>irreducible</u> over $\mathbb{Q}$.

<u>Exercise</u> Complete the factorization:

$$\underbrace{x^3+y^3+z^3-3xyz} = (\underline{x+y+z})(\qquad\qquad)$$

homogeneous degree 3

"<u>symmetric</u>"

xy^2+yz^2 <u>not</u> symmetric.

Polynomials in 1 variable

Does $p(x) = x^3 - 3x^2 + 4x - 2$ factor over $\mathbb{Q}$?

Note: $p(1) = 1 - 3 + 4 - 2 = 0$: 1 is a root of $p(x)$.

$\Rightarrow$ $x - 1$ is a factor.

$$
\begin{array}{r|llll}
 & x^2 & -2x & +2 & \\
\hline
x-1 & x^3 & -3x^2 & +4x & -2 \\
 & \cancel{x^3} & -x^2 & & \\
\hline
 & & -2x^2 & +4x & \\
 & & -\cancel{2x^2} & +2x & \\
\hline
 & & & 2x & -2 \\
 & & & \cancel{2x} & -\cancel{2} \\
\hline
 & & & & 0 \leftarrow \text{remainder}
\end{array}
$$

So $x^3 - 3x^2 + 4x - 2 = (x-1)\underbrace{(x^2 - 2x + 2)}_{\text{irreducible (over } \mathbb{Q})}$

In general, if $p(x)$, $q(x)$ are polynomials, we can do long division as above to write

$$p(x) = q(x)\,t(x) + r(x)$$

where the remainder $r(x)$ has <u>smaller degree</u> than $q(x)$.

<u>Example</u> Divide $2x^3+1$ into x^7+7x^2+3.

$$
\begin{array}{r|l}
 & \tfrac{1}{2}x^4 - \tfrac{1}{4}x \\
\hline
\underset{\text{deg } 3}{2x^3+1} & \cancel{x^7} + 0 \cdots \qquad + 7x^2 + 3 \\
 & \cancel{x^7} + \tfrac{1}{2}x^4 \\
\hline
 & -\tfrac{1}{2}x^4 + 0 \\
 & -\tfrac{1}{2}x^4 - \tfrac{1}{4}x \\
\hline
 & \underbrace{\tfrac{1}{4}x + 7x^2 + 3.}_{\substack{\text{deg } 2 \\ \| \\ \text{remainder}}}
\end{array}
$$

Conclusion

$$x^7+7x^2+3 = \left(\tfrac{1}{2}x^4 - \tfrac{1}{4}x\right)\underset{\substack{\uparrow \\ \text{cubic}}}{\left(2x^3+1\right)} + \underbrace{7x^2 + \tfrac{1}{4}x + 3}_{\text{remainder}}$$

Let $p(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$

be a polynomial of degree d. ($a_d \neq 0$)

Let s be any number.

Divide $p(x)$ by $x - s$, I get

$$p(x) = (x-s)\,t(x) + \underset{\substack{\uparrow \\ (\text{degree } 0 \,=\, \text{const})}}{r}$$

Let $x = s$: $p(s) = 0 \cdot t(s) + r = r$.

So $\boxed{p(x) = (x-s)\,t(x) + p(s).}$

This shows: $x - s$ is a factor of $p(x)$

$\Longleftrightarrow$ s is a root.

Suppose $s_1 \neq s_2$ are roots of $p(x)$.

Then $p(x) = (x - s_1)\,p_1(x)$.

$\therefore$ $0 = p(s_2) = \underset{\substack{\neq \\ 0}}{(s_2 - s_1)}\, p_1(s_2)$

$\Rightarrow p_1(s_2) = 0. \Rightarrow p_1(x) = (x - s_2)\,p_2(x)$

$\therefore$ $p(x) = (x - s_1)(x - s_2)\,p_2(x)$.

If $s_1, \ldots, s_m$ are distinct roots, then

$$p(x) = (x_1 - s_1)(x - s_2) \cdots (x - s_m)\,t(x).$$

If $p(x)$ has degree d, and if
$s_1, \dots, s_d$ are distinct roots of $p(x)$

then $p(x) = (x-s_1)(x-s_2)\dots(x-s_d)\,c$

$$a_d x^d + \cdots = c x^d + \cdots$$

[polynomial of degree 0 = const]

In fact, we must have
$c = a_d$ = coeff of x^d in $p(x)$.

Corollary Suppose $p(x)$ has degree d and distinct roots $s_1, s_2, \dots, s_d$.

Then $p(x) \mid q(x) \iff s_1, \dots, s_d$ are roots of $q(x)$.

Exercise (Shortlisted for the 1988 I.M.O)

Show x^2+x+1 divides $x^{2k}+1+(x+1)^{2k}$ if and only if k is not a multiple of 3.

---

kevin.hutchinson@ucd.ie