

The division algorithm for polynomials: If $a(x)$ and $b(x)$ are polynomials, with b not equal to 0, then there exist unique polynomials $q(x)$ and $r(x)$ such that

$$a(x) = b(x)q(x) + r(x)$$

with $\deg r(x) < \deg b(x)$.

quotient

remainder

Theorem: Any polynomial can be written uniquely (up to scalar multiple) as a product of irreducible polynomials.

Proof: Clearly, any polynomial can be written as a product of irreducibles: If it isn't irreducible already, split it into two smaller factors. Inductively, those smaller factors are products of irreducibles.

We'll prove uniqueness by induction on $\deg(f)$.
Linear polynomials are already irreducible.

Case 2: None of the $r_i(x)$ are 0.

Since $\deg r_i < \deg b_n \leq \deg a_i$, we know that the r_i 's are smaller than the a_i .

We have:

$$(q_1^{b_n+r_1})(q_2^{b_n+r_2}) \dots (q_m^{b_n+r_m}) = b_1 b_2 \dots b_n.$$

$$b_n^{*}(\text{stuff}) + r_1 r_2 \dots r_m = (b_1 b_2 \dots b_{\{n-1\}}) b_n$$

So b_n divides $r_1 r_2 \dots r_m$.

Now, b_n is irreducible, and $\deg r_i < \deg a_i$, so by induction, we have unique factorization of the product $r_1 r_2 \dots r_m$.

In particular, b_n must divide some r_i .

But $\deg r_i < \deg b_n$, so this means $r_i = 0$, we are back in Case 1.

Suppose that the factorization of f is not unique.

$$\text{Suppose that } f(x) = \underline{a_1(x) a_2(x) \dots a_m(x)} = \underline{b_1(x) b_2(x) \dots b_n(x)}.$$

Let $b_n(x)$ have the smallest degree of the a_i 's and b_j 's.

We can write $a_i(x) = q_i(x) b_n(x) + r_i(x)$ for some q_i and r_i .

Case 1: One of the r_i 's is 0.

In this case, $b_n(x) \mid a_i(x)$. Since $a_i(x)$ is irreducible, this means that $b_n(x) = a_i(x)$ up to a scalar.

Cancel $a_i(x)$ from the LHS and $b_n(x)$ from the RHS and get $a_1(x) a_2(x) \dots a_{\{i-1\}}(x) a_{\{i+1\}}(x) \dots a_m(x) = b_1(x) b_2(x) \dots b_{\{n-1\}}(x)$.

Inductively, these factorizations are equal, so the original factorizations matched.

Consequence: Let $f(x)$ and $g(x)$ be polynomials of degrees a and b with no common factor. Then there does not exist any solution, other than $u(x) = v(x) = 0$, to the equations

$$f(x) u(x) = g(x) v(x)$$

with $\deg u < b$ and $\deg v < a$.

If we take $u = g$ and $v = f$, then we have

$f(x) u(x) = g(x) v(x)$. But then $\deg u(x) = b$ and $\deg v(x) = a$.

If there were a common factor, $h(x)$, then we could take $u(x) = f(x)/h(x)$ and $v(x) = g(x)/h(x)$.

Proof: If $f(x) u(x) = g(x) v(x)$ then every irreducible factor of $g(x)$ must also appear in $u(x)$. So $g(x) \mid u(x)$, and $\deg u(x) \geq \deg g(x) = b$.

Similarly, every irred factor of $f(x)$ must appear in $v(x)$, so $f(x) \mid v(x)$ and $\deg v(x) \geq \deg f = a$.

In other words, if

$$(x^2+1) u(x) = (x^3-2) v(x),$$
 then

we must have $\deg(v) \geq 2$ and $\deg u \geq 3$.