Greatest common divisor

Let $\varphi(x), f(x), g(x)$ be polynomials in $\mathbb{F}[x]$. If $\varphi(x)$ divides both $f(x)$ and $g(x)$, then $\varphi(x)$ is called a common divisor of $f(x)$ and $g(x)$.

Def 1 Let $f(x)$ and $g(x)$ be two polynomials in $\mathbb{F}[x]$. A polynomial $d(x)$ in $\mathbb{F}[x]$ is called a greatest common divisor of $f(x)$ and $g(x)$, if it satisfies the following conditions: g.c.d.

(i) $d(x)$ is a common divisor of $f(x)$ and $g(x)$; $d(x)\mid f(x)$, $d(x)\mid g(x)$

(ii) $d(x)$ is divisible by every common divisor of $f(x)$ and $g(x)$.

If $\varphi(x)\mid f(x)$ and $\varphi(x)\mid g(x)$, then $\varphi(x)\mid d(x)$.

For example, for arbitrary polynomial $f(x)$, $f(x)$ is a greatest common divisor of $f(x)$ and 0; If $g(x)\mid f(x)$, then $g(x)$ is a greatest common divisor of $f(x)$ and $g(x)$.

Lemma 1. If $f(x)=q(x)g(x)+r(x)$, then the list of common divisors of $f(x)$ and $g(x)$ coincides with the list of common divisors of $g(x)$ and $r(x)$.

(Here insert the Euclidean Algorithm)

Theorem 1 (Bézout). For any polynomials $f(x)$ and $g(x)$ in $\mathbb{F}[x]$, there exists a greatest common divisor $d(x)$ in $\mathbb{F}[x]$, and $d(x)$ can be represented as a linear combination of $f(x)$ and $g(x)$, namely, there exist polynomials $u(x)$ and $v(x)$ in $\mathbb{F}[x]$ such that

$$d(x)=u(x)f(x)+v(x)g(x).$$ (Bézout's identity)

Example. For the pair of polynomials $f(x)$ and $g(x)$ below, use the Euclidean algorithm to find polynomials $u(x)$ and $v(x)$ such that $u(x)f(x)+v(x)g(x)$ equals a greatest common divisor of $f(x)$ and $g(x)$:

① $f(x)=x^5+1$ and $g(x)=x^2+1$ in $\mathbb{Q}[x]$;

② $f(x)=x^4+3x^3-x^2-4x-3$, and $g(x)=3x^3+10x^2+2x-3$ in $\mathbb{C}[x]$. (Exercise)

Euclidean Algorithm: Given two polynomials $f(x)$ and $g(x)$ with $g(x) \neq 0$, divide g into f, then the remainder into g, then that remainder into the previous remainder, etc, or symbolically,

$$f(x) = q_1(x)\, g(x) + r_1(x)$$
$$g(x) = q_2(x)\, r_1(x) + r_2(x)$$
$$r_1(x) = q_3(x)\, r_2(x) + r_3(x)$$
$$\vdots$$
$$r_{k-2}(x) = q_k(x)\, r_{k-1}(x) + r_k(x)$$
$$r_{k-1}(x) = q_{k+1}(x)\, r_k(x) + 0$$

Since $\deg r_1(x) < \deg g(x)$, $\deg r_2(x) < \deg r_1(x)$, etc., the sequence of divisions ends after at most $\deg g(x) = k$ steps. Then we have

Theorem: In Euclid's Algorithm for $f(x)$ and $g(x)$, the last nonzero remainder $r_k(x)$ is a greatest common divisor of f and g.

Example. Find a greatest common divisor of $f(x)$ and $g(x)$ by Euclid's Algorithm, where $f(x) = x^5+1$ and $g(x) = x^2+1$ in $\mathbb{Q}[x]$.

Solution: $f(x) = x^5+1 = (x^3-x)\, g(x) + (x+1)$

$$g(x) = (x-1)(x+1) + 2$$
$$x+1 = \tfrac{1}{2}(x+1)\cdot 2 + 0$$

This gives that 2 is a greatest common divisor of $f(x)$ and $g(x)$. □

Answers.

(1) By the Euclidean algorithm, we have the following sequence of equalities:

$$f(x) = x^5+1 = (x^3-x)g(x) + \underbrace{(x+1)}_{r_1}$$

$$g(x) = x^2+1 = (x-1)\underbrace{(x+1)}_{r_1} + \underbrace{2}_{r_2}$$

$$\underbrace{x+1}_{r_1} = \left(\tfrac{1}{2}x+\tfrac{1}{2}\right)\times \underbrace{2}_{r_2} + 0$$

The last nonzero remainder is 2. Thus 2 is a greatest common divisor of $f(x)=x^5+1$ and $g(x)=x^2+1$. Bézout theorem asserts in this case 2 is a linear combination of x^5+1 and x^2+1. Indeed, we have

$$\begin{aligned} 2 &= g(x) - (x-1)(x+1) \\ &= g(x) - (x-1)\left[f(x) - (x^3-x)g(x)\right] \\ &= \left((x-1)(x^3-x)+1\right)g(x) - (x-1)f(x) \end{aligned}$$

Hence we can take

$$u(x) = -(x-1) \quad \text{and} \quad v(x) = (x-1)(x^3-x)+1$$

which satisfy

$$2 = u(x)f(x) + v(x)g(x).$$

(2) $|9x+27|$ is a greatest common divisor of $f(x)$ and $g(x)$. And

$$|9x+27| = u(x)f(x) + v(x)g(x)$$

where $u(x) = \frac{27}{5}x - 9$ and $v(x) = -\frac{9}{5}x^2 + \frac{18}{5}x$.

The greatest common divisor is determined up to a nonzero constant multiple.

Remark: The greatest common divisors of two polynomials $f(x)$ and $g(x)$ are all non-zero constant multiples of each other. We use (f,g) or $(f(x),g(x))$ to denote the greatest common divisor with leading coefficient 1. (Uniquely determined)

For instance, if $|9x+27|$ is a g.c.d. of $f(x)$ and $g(x)$, then

$$(f,g) = x+3.$$

Def2 If the greatest common divisor of two polynomials $f(x)$ and $g(x)$ is equal to 1, then $f(x)$ and $g(x)$ are said to be relatively prime or coprime.

Thm2 Let $f(x)$ and $g(x)$ be in $F[x]$. $f(x)$ and $g(x)$ are coprime if and only if there exist $u(x), v(x) \in F[x]$ such that

$$u(x)f(x) + v(x)g(x) = 1$$

proof: It suffices to prove the sufficiency. suppoe that $d(x)$ is a greatest common divisor of $f(x)$ and $g(x)$. Then $d(x) | f(x)$ and $d(x) | g(x)$. Thus $d(x)$ divides 1. This implies $d(x)$ is a non-zero constant. Hence, $f(x)$ and $g(x)$ are coprime. □

Corollary 1 If $(f(x), g(x)) = 1$ and $f(x) | g(x)h(x)$, then $f(x) | h(x)$.

proof: There exist $u(x)$ and $v(x)$ such that

$$u(x)f(x) + v(x)g(x) = 1.$$

Then multiplying both sides of the equation by $h(x)$ yields

$$u(x)f(x)h(x) + v(x)g(x)h(x) = h(x).$$

It follows $f(x) | h(x)$, since $f(x)$ divides the left-hand side of the equation. □.

Corollary 2 If $f_1(x) | g(x)$, $f_2(x) | g(x)$ and $(f_1(x), f_2(x)) = 1$, then $f_1(x)f_2(x) | g(x)$.

proof: By $f_1(x) | g(x)$, there exists $h(x)$ such that

$$g(x) = f_1(x)h(x)$$

Now $f_2(x) | f_1(x)h(x)$ and $(f_1(x), f_2(x)) = 1$, thus $f_2(x) | h(x)$. There exists $h_2(x)$ such that

$$h(x) = f_2(x)h_2(x)$$

This gives $g(x) = f_1(x)f_2(x)h_2(x)$ and thus $f_1(x)f_2(x) | g(x)$. □

Generalizations to more than two polynomials.

Def3. Let $f_1(x), f_2(x), \cdots, f_s(x)$ $(s \geq 2)$ be polynomials in $F[x]$. A polynomial $d(x)$ in $F[x]$ is called a greatest common divisor of $f_1, f_2, \cdots, f_s$ if it satisfies

1) $d(x) \mid f_i(x)$, $1 \leq i \leq s$;

2) if $h(x) \mid f_i(x)$, $1 \leq i \leq s$, then $h(x) \mid d(x)$.

We still use $(f_1, f_2, \cdots, f_s)$ to denote the greatest common divisor whose leading coefficient is equal to 1. If $f_1(x), \cdots, f_s(x)$ are non-zero polynomials, then

$$(f_1, f_2, \cdots, f_s) = ((f_1, f_2, \cdots, f_{s-1}), f_s).$$

Furthermore, there exist polynomials $u_i(x)$, $1 \leq i \leq s$, such that

$$u_1(x)f_1(x) + u_2(x)f_2(x) + \cdots + u_s(x)f_s(x) = (f_1, f_2, \cdots, f_s).$$

Def4. Polynomials $f_1(x), \cdots, f_s(x)$ $(s \geq 2)$ whose greatest common divisor $(f_1, f_2, \cdots, f_s)$ is equal to 1 are said to be relatively prime or coprime.

Homework:

P29. 5, 6, 7, 8, 9, 10, 11, 12, 13, 14.

Appendix (I) The method of mathematical induction

Theorem 1. (Induction) Fix an integer n_0 and let $P(n)$ be a statement which makes sense for every integer $n \geq n_0$. Then $P(n)$ is true for all $n \geq n_0$, if the following two statements are true:

(a) $P(n_0)$ is true;

(b) for all $k \geq n_0$, if $P(k)$ is true, then $P(k+1)$ is true.

When using induction to prove a theorem, proving (a) is called the base case, and proving (b) is called the induction step.

~~proof: Let $sp(n)$ be ...~~

Example 1. For all $n \geq 1$, $1+3+5+\cdots+(2n-1)=n^2$.

proof: Let $P(n)$ be the statement

$$1+3+5+\cdots+(2n-1)=n^2$$

The base case $P(1)$ is true, since $1=1^2$. For the induction step, let k be some unspecified number ≥ 1, and assume that $P(k)$ is true, that is,

$$1+3+5+\cdots+(2k-1)=k^2.$$

We want to show that then $P(k+1)$ is true, that is,

$$1+3+\cdots+(2k-1)+(2k+1)=(k+1)^2.$$

To do so, we can add $(2k+1)$ to both sides of the equation $P(k)$ to get

$$1+3+\cdots+(2k-1)+(2k+1)=k^2+(2k+1)=(k+1)^2$$

Thus, assuming $P(k)$ is true, it follows that $P(k+1)$ is true.

By induction, $P(n)$ is true for all ~~$n \geq 1$~~ $n \geq 1$. □

Theorem 2 (Complete Induction) Let n_0 be a fixed integer and let $P(n)$ be a statement which makes sense for every integer $n \geq n_0$. Then $P(n)$ is true for all integers $n \geq n_0$, if the following two statement are true:

(a) (base case) $P(n_0)$ is true;

(b) (induction step) For all $m > n_0$, if $P(k)$ is true for all $n_0 \leq k < m$, then $P(m)$ is true.

Example 2 Every natural number $n \geq 2$ is divisible by a prime number.

Proof. Let $P(n)$ be the statement "n is divisible by a prime number, where $n \geq 2$." Then the base case $P(2)$ is true, because 2 is prime and 2 divides itself. We'll use complete induction for the induction step. Thus we assume $P(k)$ is true for all k where $2 \leq k < m$: that is, we assume that every natural number ≥ 2 and $< m$ is divisible by a prime number. Now consider m. If m is prime, then m is divisible by a prime number, namely, itself, and $P(m)$ is true. If m is not prime, then m factors as $m = ab$, where $2 \leq a < m$ and also $2 \leq b < m$. Since $2 \leq a < m$, by assumption $P(a)$ is true, that is, a is divisible by a prime. Since a is divisible by a prime, and a divides m, m is divisible by the same prime. So $P(m)$ is true.

Thus $P(n)$ is true for all $n \geq 2$ by Complete Induction. □