<u>הגדרה 1.</u> פולינום $d(x)\in F[x]$ נקרא <u>מחלק משותף</u> של הפולינומים $f(x),g(x)\in F[x]$ אם $(d(x)\mid f(x))\wedge(d(x)\mid g(x))$. קבוצהת כל המחלקים המשותפים של $f(x),g(x)\in F[x]$ תסומן כ- $\mathrm{Div}(f(x),g(x))$.

אם לפחות אחד מהפולינומים $f(x),g(x)$, נגיד $f(x)$, שונה מאפס, אז המעלה של כל מחלק משותף שלהם מוגבלת ע"י $\deg(f(x))$. לכן תמיד אפשר לבחור מחלק משותף $d(x)\in\mathrm{Div}(f(x),g(x))$ בעל מעלה מקסימלית. כל מחלק משותף בעל מעלה מקסימלית נקרא <u>מחלק משותף הגדול ביותר</u> (קיצור - מ.מ.ג) של הפולינומים $f(x),g(x)$.

<u>טענה 1.</u> אם $h(x)\in F[x]$ הוא מ.מ.ג. של פולינומים $g(x),f(x)\in F[x]$, אז גם $ah(x),a\in F\setminus\{0\}$ מ.מ.ג. של אותם הפולינומים.

<u>הוכחה.</u>

$h(x)\mid f(x)\wedge h(x)\mid g(x)\Rightarrow(ah(x))\mid f(x)\wedge(ah(x))\mid g(x)$. לכן $ah(x)$ מחלק משותף של $f(x),g(x)$. מהשוויון $\deg(ah(x))=\deg(h(x))$ נובע ש- $ah(x)$ בעל מעלה מקסימלית בין המחלקים משותפים. מכאן נובע $ah(x)$ מ.מ.ג. של $f(x),g(x)$.
מ.ש.ל.

מהטענה הנ"ל נובע שאם $d(x)$ מחלק משותף גדול ביותר של $f(x),g(x)$ אז כל פולינום הפרופורציונאלי ל- $d(x)$ גם יהיה מחלק משותף גדול ביותר של אותם הפולינומים. לכן מחלק משותף גדול ביותר אינו יחיד.

<u>טענה 2.</u> אם $h(x)\in F[x]$ הוא מחלק משותף של הפולינומים $g(x),f(x)\in F[x]$, אז הוא מחלק כל צירוף ליניארי $u(x)\cdot g(x)+v(x)\cdot f(x),\ u(x),v(x)\in F[x]$ שלהם.

<u>הוכחה.</u>

מהגדרת ההתחלקות נובע שקיימים $b(x),b(x)\in F[x]$ כך ש:

$$f(x)=h(x)\cdot a(x),\ g(x)=h(x)\cdot b(x)$$

מכאן נובע ש:

$$u(x)\cdot g(x)+v(x)\cdot f(x)=(u(x)\cdot b(x)+v(x)\cdot a(x))\cdot h(x).$$

הפולינום $u(x)\cdot b(x)+v(x)\cdot a(x)$ שייך ל- $F[x]$, לכן $h(x)\mid u(x)\cdot g(x)+v(x)\cdot f(x)$.
מ.ש.ל.

<u>טענה 3.</u> לכל שני פולינומים $f(x),g(x)\in F[x],g(x)\neq 0(x)$ מתקיים $\mathrm{Div}(f(x),g(x))=\mathrm{Div}(g(x),r(x))$ כאשר $r(x)$ הוא שארית החילוק $f(x)$ ב- $g(x)$.
בפרט, כל מ.מ.ג. של $f(x),g(x)$ הוא מ.מ.ג של $g(x),r(x)$, ולהפך.

<u>הוכחה.</u>

מהגדרה של $r(x)$ נובע ש- $r(x)=f(x)-g(x)\cdot q(x)$.
ניקח מחלק משותף $h(x)$ של הפולינומים $f(x)$ ו $g(x)$. מטענה 2 נובע ש- $h(x)$ מחלק $r(x)$. לכן $h(x)\in\mathrm{Div}(g(x),r(x))\Leftarrow\big(h(x)\mid g(x)\big)\wedge\big(h(x)\mid r(x)\big)$.
נניח עכשיו ש- $h(x)\in\mathrm{Div}(g(x),r(x))$. לפי טענה 2 $h(x)$ מחלק את $f(x)$ (כי $f(x)=r(x)+g(x)\cdot q(x)$ צירוף ליניארי של $r(x),g(x)$). לכן

$$h(x)\in\mathrm{Div}(g(x),f(x))\Leftarrow\big(h(x)\mid g(x)\big)\wedge\big(h(x)\mid f(x)\big)$$

מ.ש.ל.

<u>טענה 4.</u> יהיו $f(x),g(x)\in F[x],g(x)\neq 0(x)$ שני פולינומים כלשהם, אז:

א. קיים מ.מ.ג. $h(x)$ שלהם שניתן להציג אותו כצירוף ליניארי

$$d(x)=u(x)\cdot f(x)+v(x)\cdot g(x),u(x),v(x)\in F[x]$$.

ב. כל מחלק משותף של $f(x),g(x)$ מחלק את $d(x)$.

ג. כל מחלק משותף הגדול ביותר של $f(x),g(x)$ פרופורציונאלי ל-$d(x)$.

<u>הוכחה.</u>

<u>א'+ב'</u>

נביט בקבוצה $S\subseteq F[x]$ של כל הצירופים הליניאריים

$$d(x)=u(x)\cdot f(x)+v(x)\cdot g(x),u(x),v(x)\in F[x]$$

של $f(x),g(x)$ השונים מפולינום-אפס. הקבוצה S לא ריקה, מפני ש-$g(x)\in S$.
לכן אפשר לבחור פולינום $d(x)\in S$ בעל מעלה מינימלית. נוכיח ש-$d(x)$ מ.מ.ג של הפולינומים $f(x),g(x)$. נזכיר ש-$d(x)=u(x)\cdot f(x)+v(x)\cdot g(x)$ עבור $u(x),v(x)\in F[x]$ מסוימים.

<u>1. $(d(x)\mid f(x))\wedge(d(x)\mid g(x))$.</u>

נחלק $g(x)$ ב-$d(x)$ עם שארית: $g(x)=d(x)\cdot q(x)+r(x),\deg(r(x))<\deg(d(x))$.
אז נקבל

$$\begin{aligned}r(x)=\ & g(x)-d(x)\cdot q(x)\ =\\ & g(x)-q(x)\cdot(u(x)\cdot f(x)+v(x)\cdot g(x))=\\ & g(x)\cdot(1-q(x)\cdot v(x))+u(x)\cdot f(x)\end{aligned}$$

כלומר $r(x)$ הוא צירוף ליניארי של $f(x),g(x)$. אם $r(x)\neq 0(x)$, אז $r(x)\in S$ ו-$\deg(r(x))<\deg(d(x))$ בניגוד לבחירה של $d(x)$ ($d(x)$ נבחר כבעל מעלה מינימלית). סתירה, לכן $r(x)=0(x)$ ו-$d(x)$ מחלק את $g(x)$.
באופן דומה ניתן להוכיח ש-$d(x)$ מחלק את $f(x)$.

<u>2. כל מחלק משותף של $f(x),g(x)$ מחלק את $d(x)$.</u>

אם $h(x)$ מחלק משותף של $f(x),g(x)$ אז הוא מחלק כל צירוף ליניארי שלהם (טענה 2). לכן $h(x)\mid d(x)$.

<u>3. $d(x)$ בעל מעלה מקסימלית בין כל המחלקים המשותפים.</u>

מחלק 2 נובע שכל מחלק משותף $h(x)$ של $f(x),g(x)$ מחלק את $d(x)$, לכן $\deg(h(x))\leq\deg(d(x))$.

<u>ג.</u>

אם $h(x)$ מ.מ.ג. כלשהו של $f(x),g(x)$, אז, לפי סעיף ב', $h(x)\mid d(x)$. מצד שני, $h(x)$ בעל מעלה מקסימלית בין כל המחלקים המשותפים. לכן $\deg(h(x))=\deg(d(x))$. מכאן נובע שבשוויון $d(x)=h(x)\cdot a(x)$ הפולינום $a(x)$ הוא פולינום ממעלה אפס. לכן $d(x)=h(x)\cdot(a_0x^0)=a_0h(x)$ (מקדם a_0 שונה מאפס מפני ש-$d(x)\neq 0(x)$).

מ.ש.ל.

יהי $d(x)=d_mx^m+\ldots+d_0,d_m\neq 0$ מחלק משותף הגדול ביותר של שני פולינומים $f(x),g(x)$. מטענה 1 נובע ש-$d_m^{-1}d(x)$ גם הוא מחלק משותף הגדול ביותר של

אותם הפולינומים. $d_m^{-1}d(x)$ הוא פולינום מתוקן. מטענה 4 נובע שכל שני מחלקים משותפים הגדולים ביותר של $f(x),g(x)$ פרופורציונאליים זה לזה. שני פולינומים מתוקנים פרופורציונאליים זה לזה אם ורק אם הם שווים. לכן <u>לכל שני פולינומים</u> <u>$f(x),g(x)$ קיים מ.מ.ג. יחיד שהוא פולינום מתוקן.</u> לפולינום הזה ניקרא <u>המחלק המשותף הגדול ביותר</u> של $f(x),g(x)$ ונסמן אותו כ- $\gcd(f(x),g(x))$.

מטענה 3 נובע ש- $\gcd(f(x),g(x))=\gcd(g(x),r(x))$ כאשר $r(x)$ הוא שארית החילוק של $f(x)$ ב- $g(x)$. השוויון הזה הוא בסיס של אלגוריתם אוקלידס לחישוב $\gcd(f(x),g(x))$.

נתונים שני פולינומים $f(x),g(x),\deg(f(x))\geq\deg(g(x)),f(x)\neq 0(x)$. יש למצוא $\gcd(f(x),g(x))$.

1. אתחול: $\gcd(f(x),g(x)):=f(x)$.
2. אם $g(x)=0(x)$ אז "GOTO 4".
3. מצא את השארית $r(x)$ של החילוק $f(x)$ ב- $g(x)$.
   $f(x):=g(x),g(x):=r(x)$ ו "GOTO 2".
4. לעצור.