יהי p ראשוני. $\deg$ על $\mathbb{Q}$ מקנה פולינום $f(x)\in\mathbb{Z}[x]$ שהוא פרימיטיבי.

הגדרה: פולינום $f(x)\in\mathbb{Z}[x]$ נקרא **פרימיטיבי** אם ה-$\gcd$ של כל מקדמיו הוא 1.

למה (גאוס): מכפלת שני פולינומים פרימיטיביים היא פרימיטיבית.

מסקנה: יהי $f(x)\in\mathbb{Z}[x]$ פרימיטיבי. אז f פריק מעל $\mathbb{Q}[x]$ אם ורק אם f פריק ב-$\mathbb{Z}[x]$.

דוגמה: $f(x)=x^4+x^2+1$ אי-פריק ב-$\mathbb{Z}[x]$.

נבדוק מודולו $p=2$: $f(x)=x^4+x^2+1$ אי-פריק ב-$\mathbb{Z}_2[x]$ כי $f(0)=f(1)=1\neq 0$.

עבור $p=3$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=5$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=7$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=11$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=13$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=17$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=19$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=23$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=29$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=31$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=37$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=41$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=43$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=47$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=53$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=59$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=61$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=67$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=71$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=73$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=79$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=83$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=89$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=97$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=101$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=103$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=107$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=109$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=113$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=127$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=131$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=137$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=139$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=149$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=151$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=157$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=163$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=167$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=173$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=179$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=181$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=191$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=193$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=197$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=199$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=211$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=223$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=227$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=229$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=233$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=239$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=241$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=251$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=257$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=263$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=269$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=271$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=277$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=281$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=283$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=293$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=307$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=311$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=313$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=317$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=331$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=337$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=347$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=349$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=353$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=359$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=367$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=373$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=379$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=383$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=389$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=397$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=401$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=409$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=419$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=421$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=431$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=433$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=439$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=443$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=449$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=457$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=461$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=463$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=467$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=479$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=487$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=491$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=499$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=503$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=509$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=521$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=523$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=541$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=547$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=557$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=563$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=569$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=571$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=577$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=587$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=593$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=599$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=601$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=607$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=613$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=617$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=619$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=631$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=641$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=643$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=647$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=653$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=659$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=661$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=673$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=677$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=683$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=691$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=701$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=709$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=719$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=727$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=733$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=739$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=743$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=751$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=757$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=761$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=769$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=773$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=787$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=797$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=809$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=811$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=821$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=823$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=827$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=829$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=839$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=853$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=857$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=859$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=863$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=877$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=881$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=883$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=887$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=907$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=911$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=919$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=929$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=937$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=941$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=947$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=953$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=967$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=971$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=977$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=983$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=991$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=997$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1009$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1013$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1019$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1021$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1031$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1033$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1039$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1049$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1051$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1061$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1063$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1069$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1087$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1091$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1093$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1097$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1103$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1109$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1117$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1123$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1129$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1151$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1153$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1163$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1171$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1181$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1187$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1193$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1201$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1213$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1217$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1223$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1229$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1231$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1237$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1249$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1259$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1277$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1279$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1283$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1289$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1291$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1297$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1301$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1303$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1307$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1319$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1321$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1327$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1361$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1367$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1373$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1381$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1399$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1409$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1423$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1427$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1429$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1433$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1439$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1447$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1451$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1453$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1459$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1471$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1481$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1483$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1487$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1489$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1493$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1499$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1511$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1523$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1531$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1543$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1549$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1553$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1559$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1567$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1571$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1579$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1583$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1597$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1601$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1607$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1609$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1613$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1619$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1621$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1627$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1637$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1657$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1663$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1667$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1669$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1693$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1697$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1699$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1709$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1721$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1723$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1733$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1741$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1747$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1753$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1759$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1777$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1783$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1787$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1789$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1801$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1811$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1823$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1831$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1847$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1861$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1867$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1871$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1873$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1877$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1879$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1889$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1901$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1907$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1913$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1931$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1933$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1949$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1951$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1973$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1979$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1987$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1993$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=1997$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=1999$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2003$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2011$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2017$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2027$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2029$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2039$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2053$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2063$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2069$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2081$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2083$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2087$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2089$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2099$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2111$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2113$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2129$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2131$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2137$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2141$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2143$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2153$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2161$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2179$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2203$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2207$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2213$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2221$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2237$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2239$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2243$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2251$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2267$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2269$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2273$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2281$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2287$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2293$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2297$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2309$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2311$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2333$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2339$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2341$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2347$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2351$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2357$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2371$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2377$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2381$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2383$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2389$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2393$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2399$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2411$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2417$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2423$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2437$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2441$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2447$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2459$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2467$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2473$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2477$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2503$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2521$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2531$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2539$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2543$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2549$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2551$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2557$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2579$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2591$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2593$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2609$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2617$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2621$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2633$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2647$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2657$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2659$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2663$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2671$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2677$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2683$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2687$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2689$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2693$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2699$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2707$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2711$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2713$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2719$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2729$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2731$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2741$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2749$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2753$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2767$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2777$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2789$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2791$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2797$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2801$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2803$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2819$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2833$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2837$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2843$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2851$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2857$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2861$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2879$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2887$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2897$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2903$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2909$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2917$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2927$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2939$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2953$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2957$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2963$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2969$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=2971$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=2999$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3001$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3011$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3019$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3023$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3037$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3041$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3049$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3061$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3067$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3079$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3083$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3089$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3109$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3119$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3121$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3137$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3163$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3167$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3169$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3181$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3187$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3191$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3203$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3209$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3217$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3221$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3229$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3251$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3253$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3257$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3259$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3271$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3299$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3301$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3307$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3313$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3319$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3323$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3329$: $f(x)=x^4+x^2+1$ אי-פריק.

עבור $p=3331$: $f(x)=x^4+x^2+1$ פריק.

עבור $p=3343$: $f(x)=x^4+x^

□ המסקנה נובעת.

מלמה של Gauss: $f*g$ פרימיטיבי $\Leftarrow$ f ו-g פרימיטיביים. יהי p ראשוני. נסתכל על $\mathbb{Z}_p[x]$.
$(f*g)(x) = \sum_{i+j=x} a_i b_j$. אם $p \nmid a_i$ לכל i אז f פרימיטיבי, ואם $p \nmid b_j$ לכל j אז g פרימיטיבי.
נניח בשלילה ש-$p \mid a_i$ לכל i וגם $p \mid b_j$ לכל j. אז $(f*g)(x) = 0$ ב-$\mathbb{Z}_p[x]$, כלומר $p \mid c_k$ לכל k.
$\Rightarrow$ $f*g$ אינו פרימיטיבי.

□

הוכחה: $f = \frac{a}{b} f_1$, $f_1 \in \mathbb{Z}[x]$ פרימיטיבי. $g = \frac{c}{d} g_1$, $g_1 \in \mathbb{Z}[x]$ פרימיטיבי.
$f*g = \frac{ac}{bd} (f_1 * g_1)$. $f_1 * g_1$ פרימיטיבי $\Rightarrow$ $\gcd$ של המקדמים הוא 1.
$\Rightarrow$ $\frac{ac}{bd}$ הוא המקדם המוביל של $f*g$.

□

מסקנה: יהי $f \in \mathbb{Z}[x]$ פולינום פרימיטיבי. אם $f = gh$ ב-$\mathbb{Q}[x]$ אז $f = g_1 h_1$ ב-$\mathbb{Z}[x]$ כאשר $\deg g_1 = \deg g$, $\deg h_1 = \deg h$.

הוכחה: $f = \frac{a}{b} g_1 h_1$, $g_1, h_1 \in \mathbb{Z}[x]$ פרימיטיביים. $bf = a g_1 h_1$.
$p \mid b$ ראשוני $\Rightarrow$ $p \mid a g_1 h_1$. f פרימיטיבי $\Rightarrow$ $p \nmid a$.
$\Rightarrow$ $p \mid g_1 h_1$. $g_1 h_1$ פרימיטיבי $\Rightarrow$ $p \nmid g_1 h_1$. סתירה.
$\Rightarrow$ $b = \pm 1$. $f = \pm g_1 h_1$.

דוגמה $n = 1$.

□

בהוכחת משפט 3 $\Leftarrow$ $\lambda = (\lambda_1, \lambda_2)$, $\lambda_1 \geq \lambda_2$ מקיים את $\lambda_1 - \lambda_2 = 1$ ו-$\lambda_1 = n$.
כיוון ש-$h(x)$ פרימיטיבי $\Leftarrow$ $\gcd$ של המקדמים $= 1$.
בהוכחת $(x)h\eta = (x)_* f \lambda$. המקדמים המובילים של λ ו-η הם 1.
נניח את $\frac{f(x)}{e} = (x)_* f$ כך ש-$\deg g = \deg h$, $e \in \mathbb{N}$. אז ב-$\mathbb{Z}[x]$ נקבל את
$$(x)h \cdot \frac{f(x)}{e} = (x)_* f .$$
$\mathbb{Z}[x] \ni h(x) \cdot g(x)$ פרימיטיבי. אז $(x)h \cdot g(x) = (x)_* f = (x)_* \eta (f)c$. לכן:
נשאר להראות שיתכן. נניח כי $h(x) \cdot e = f(x)$ הינו פרוק כלשהו כך ש-$0 < e$ וגם
$\frac{B}{Q} = (f)c$ אז $\frac{Q}{B} = (x)_* f$ ואז $\frac{Q}{B} \cdot f(x) = g(x) \in \mathbb{Z}[x]$ פולינום פרימיטיבי. מאידך
$e \in \mathbb{Z}$ כך ש-$\frac{B}{Q} > 0$.
נסמן: $Q = \pm p$ כאשר p הינו $\gcd$ של מקדמי $f(x)$, ונסמן בקבוצה כל
$\beta = b_m \cdots b_0 q = B$. אז $\beta f(x) \in \mathbb{Z}[x] = g(x)$.
הוכחה: נניח: $x^i \frac{b_i}{a_i} \sum_{i=0}^{n} = f(x)$ כאשר $a_i, b_i \in \mathbb{Z}$.
הגדרה: המספר $c(f)$ נקרא **התוכן** (content) של $f(x)$.
מסקנה מיידית: $f \in \mathbb{Q}[x] \mapsto f_*(x)$ הינו פרימיטיבי.
למה (למה של Gauss) המכפלה של שני פולינומים פרימיטיביים הוא פולינום פרימיטיבי.

הוכחה: נניח כי $f(x)g(x)$ פרימיטיבי אבל $f(x)$ לא פרימיטיבי. לכן קיים ראשוני p המחלק
את $c(f)$. נסתכל על $\mathbb{Z}_p[x]$. נגדיר: $\varphi_p : \mathbb{Z} \to \mathbb{Z}_p$, אז שארית מחלוקה ב-$p$. φ הומומורפיזם.
$\varphi_*(f) \cdot \varphi_*(g) = \varphi_*(fg) = 0$.
אז מתקיים $\varphi_*(f) \cdot \varphi_*(g) = 0$.
כאשר $\varphi_*(f) \neq 0$ וגם $\varphi_*(g) \neq 0$. סתירה. □
$\varphi_*(g) = 0$. אבל f, g פרימיטיביים, כלומר $\varphi_*(f) \neq 0$ וגם $\varphi_*(g) \neq 0$. סתירה.
כלומר שורש של f הוא $\frac{p}{q}$ כאשר $p \mid a_0$ ו-$q \mid a_n$.

3 הרצאה

הגדרה. יהי F שדה. σ אוטומורפיזם של F אם $\sigma: F \to F$ חח"ע ועל, $\sigma(a+b)=\sigma(a)+\sigma(b)$ ו- $\sigma(ab)=\sigma(a)\sigma(b)$ לכל $a,b \in F$.

הגדרה. יהי F שדה. τ הומומורפיזם של F אם $\tau: F \to F$ חח"ע, $\tau(a+b)=\tau(a)+\tau(b)$ ו- $\tau(ab)=\tau(a)\tau(b)$ לכל $a,b \in F$.

דוגמאות: $\sigma: \mathbb{Q} \to \mathbb{Q}$ הוא הומומורפיזם. נסמן $\sigma \in \mathbb{Q}$. σ הוא אוטומורפיזם של $\mathbb{Q}$ אם $\sigma(x)=x$ לכל $x \in \mathbb{Q}$.

הגדרה. יהי F שדה. τ הומומורפיזם של F אם $\tau: F \to F$ חח"ע, $\tau(a+b)=\tau(a)+\tau(b)$ ו- $\tau(ab)=\tau(a)\tau(b)$ לכל $a,b \in F$.

דוגמאות: $\sigma: \mathbb{Q} \to \mathbb{Q}$ הוא הומומורפיזם. נסמן $\sigma \in \mathbb{Q}$. σ הוא אוטומורפיזם של $\mathbb{Q}$ אם $\sigma(x)=x$ לכל $x \in \mathbb{Q}$.

$\sigma(x)=x$ לכל $x \in \mathbb{Q}$ אם σ הוא אוטומורפיזם של $\

הגדרה קיבולו: $\mathbb{F}\subseteq\mathbb{F}(\alpha_1,\dots,\alpha_n)\subseteq T$ נאמר כי $\mathbb{F}(\alpha_1,\dots,\alpha_n)$ מתקבל מ-$\mathbb{F}$ ע"י צירוף $\alpha_1,\dots,\alpha_n$.

הוכחה: נניח $f(\alpha_1,\dots,\alpha_n)\neq 0$ (אחרת נוכיח עבור $\frac{g(\alpha_1,\dots,\alpha_n)}{f(\alpha_1,\dots,\alpha_n)}$ כאשר $g\in\mathbb{F}[x_1,\dots,x_n]$ נמצא ע"י חלוקת פולינומים). נסמן $\mathbb{F}(\alpha_1,\dots,\alpha_n)$ ע"י $\mathbb{F}$ ואת $\alpha_1,\dots,\alpha_n$ ע"י $\alpha_1,\dots,\alpha_n$. $\square$

הוכחה: כל שדה K ש$\mathbb{F}\subseteq K\subseteq T$ מכיל את $\alpha_1,\dots,\alpha_n$ ולכן מכיל גם $\mathbb{F}(\alpha_1,\dots,\alpha_n)$.

למה: $\mathbb{F}(\alpha_1,\dots,\alpha_n)$ הינו תת שדה קטן ביותר המכיל את $\mathbb{F}$ ואת $\alpha_1,\dots,\alpha_n$.

הוכחה: נסמן $\mathbb{F}(\alpha_1,\dots,\alpha_n)$ ע"י $\mathbb{F}$ ואת $\alpha_1,\dots,\alpha_n$ ע"י $\alpha_1,\dots,\alpha_n$.

$$\mathbb{F}(\alpha_1,\dots,\alpha_n)=\left\{\frac{\beta}{\gamma}:\beta,\gamma\in\mathbb{F}[\alpha_1,\dots,\alpha_n],\gamma\neq 0\right\}\subseteq T$$

ע"י למה קודמת.

קל לראות כי $\mathbb{F}(\alpha_1,\dots,\alpha_n)$ תת שדה.

קל לראות ש- $\mathbb{F}(\alpha_1,\dots,\alpha_n)$ מוכל בכל תת שדה המכיל את $\mathbb{F}$ ואת $\alpha_1,\dots,\alpha_n$.

$$\mathbb{F}[\alpha_1,\dots,\alpha_n]=\{h(\alpha_1,\dots,\alpha_n):h\in\mathbb{F}[x_1,\dots,x_n]\}\subseteq T$$

הגדרה: נניח כי $\mathbb{F}\subseteq T$ הרחבה של שדות, ויהי $\alpha_1,\dots,\alpha_n\in T$. נסמן:

$\mathbb{F}(\alpha_1,\dots,\alpha_n)$ ע"י $\mathbb{F}[\alpha_1,\dots,\alpha_n]$.

סוקלידס. אוילר. אם $p=n$ ראשוני, $\Phi_p(x)=\sum_{i=0}^{n-1}x^i$.

$\mathbb{Q}$ מעל $\mathbb{Q}$ נקרא הפולינום הציקלוטומי: דרישה: מסוים $\Phi_n(x)$ דרישתו היחיד $\phi(n)$, השורשים $\mathbb{Q}$ מעל $\mathbb{Q}$ הינו אוסף כל $\omega_n^k=e^{\frac{2\pi i k}{n}}$ ביחס ל-x^n-1. הפולינום המינימלי של ω_n^k מעל $\mathbb{Q}$ נקרא הפולינום הציקלוטומי: דרישה: מסוים $\Phi_n(x)$ דרישתו היחיד $\phi(n)$, השורשים הפולינום המינימלי של ω_n^k מעל $\mathbb{Q}$ הינו אוסף כל $\omega_n^k=e^{\frac{2\pi i k}{n}}$ ביחס ל-x^n-1. הפולינום המינימלי של ω_n^k מעל $\mathbb{Q}$ נקרא הפולינום הציקלוטומי: דרישה: מסוים $\Phi_n(x)$ דרישתו היחיד $\phi(n)$, השורשים

לכן: $\deg(\Phi_{12})=\phi(12)=4$. קל לראות כי הפולינום $\Phi_{12}(x)$ מינימלי עבור $\sqrt{2}+\sqrt{3}$.

$$\Phi_{12}(x)=(x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))$$

= נסמן $1+x^2-x^4=(x)f$. נניח כי $f(x)$ אי-פריק מעל $\mathbb{Q}$, מתקיים:

הוא מה-פולינום המינימלי של $\sqrt{2}$ מעל $\mathbb{Q}$ הינו x^2-2

מסקנה: הפולינום המינימלי של $\alpha\in T$ אי-פריק מעל $\mathbb{F}$.

הגדרה: יהי $\alpha\in T$ אלגברי מעל $\mathbb{F}$, כלומר T הרחבה של $\mathbb{F}$. הפולינום שאת קיומו הוכחנו בלמה החלוקה נקרא הפולינום המינימלי של α מעל $\mathbb{F}$.

למה: נניח כי $\alpha\in T$ אלגברי מעל $\mathbb{F}$, כלומר T הרחבה של $\mathbb{F}$. אז קיים פולינום מתוקן יחיד $f\in\mathbb{F}[x]$ המקיים: 1) $f(\alpha)=0$

2) לכל $g\in\mathbb{F}[x]$ כך ש- $g(\alpha)=0$ מתקיים $f\mid g$.

יתר על כן, f פולינום כזה הוא אי פריק במעל $\mathbb{F}$.

הוכחה: יהי $g\in\mathbb{F}[x]$ פולינום כך ש- $g(\alpha)=0$. מאלגוריתם החלוקה נובע כי קיימים $r,q\in\mathbb{F}[x]$ כך ש- $g=qf+r$ כאשר $\deg r<\deg f$ או $r=0$. נציב α ונקבל $r(\alpha)=0$. מאחר שמקדם הגבוה של f שווה 1 נובע כי $f\mid g$. בדרך אחרת - נעזר בהגדרה את יחידות f. אילו היו $\tilde{f}$ מקיים את 1), 2) אז: $f\mid\tilde{f}$ ו- $\tilde{f}\mid f$, ובגלל שמקדמים מתוקנים: $\tilde{f}=f$. $\square$

דוגמאות נוספות $\mathbb{Q}$ הרחבה של $\mathbb{C}$, $x^4-2 \in \mathbb{Q}[x]$

$$x^4-2=(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-i\sqrt[4]{2})(x+i\sqrt[4]{2})$$

לכן $K=\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2})$ הוא שדה הפיצול של x^4-2.

נשים לב שמתקיים: $K=\mathbb{Q}(\sqrt[4]{2}, i) \supseteq \mathbb{Q}(i)=L$.

מצד שני $\sqrt[4]{2}\, i$ מאפסים את x^4-2, ולכן מלוה קונצי $K \supseteq T$.

ש T מכילים את x^4-2 מאפסים את T, ולכן מלוה קונצי $T \supseteq K$.

מסקנה יהי $T \supset F$ ויהי $T \ni \alpha_1, \ldots, \alpha_n$ כך ש $1 \le s \le n$. מתקיים:

$$F(\alpha_1, \ldots, \alpha_n) = (F(\alpha_1, \ldots, \alpha_s))(\alpha_{s+1}, \ldots, \alpha_n)$$

למה יהי $T \supset F$ הרחבה של שדות. יהי $T \ni \alpha$ אלגברי מעל F, ויהי $f \in F[x]$ המינימלי של α. אז קיים איזומורפיזם יחיד $\psi: F[\alpha] \to F[x]/\langle f \rangle$ שמקבוע על F ומעביר את α לקלס $x+\langle f \rangle$.

מסקנה α אי פריק $\Rightarrow \langle f \rangle$ שדה $\Rightarrow F[\alpha]$ שדה! (בניגוד ל $\mathbb{Z}$ שלמרות ש $\mathbb{Z}$)

$\psi(x)=\alpha$ כך ש $\psi: F[x] \to T$ הומומורפיזם הערכה. נזכיר כי ψ לגמרי ע"י $\psi(h)=h(\alpha)$.

הוכחת למה: נסמן $\psi: F[x] \to T$ כך ש $\psi(h)=h(\alpha)$. קל לראות כי ψ הומומורפיזם

יהי $g \in F[x]$. $g(\alpha)=0 \Leftrightarrow g(\alpha)=(fd)(\alpha)=f(\alpha)d(\alpha)=0$

~~$\ker \psi = \langle f \rangle$~~ $\ker \psi \subseteq \langle f \rangle$. יהי $g \in \ker \psi$. אז $0=\psi(g)=g(\alpha)$. מאידך $f \mid g$ (כי f מינימלי של α) ולכן $g=fh$ עבור h. מאידך $f \in \langle f \rangle$. $\Rightarrow \ker \psi \subseteq \langle f \rangle$.

ממשפט האיזומורפיזם הראשון $F[x]/\ker \psi \cong \mathrm{Im}\psi \subseteq T$ $\Rightarrow F[\alpha] \cong F[x]/\langle f \rangle$.

יחידות: נניח כי φ הומומורפיזם מ $F[\alpha]$ לתוך T שמקבוע על F ומעביר את α ל $x+\langle f \rangle$.

$\square$

תרגיל 3

תרגיל נניח כי $f(x)=\sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ ונניח כי $\frac{s}{t}$ הוא שורש של $f(x)$. כך ש $\gcd(s,t)=1$

אז $a_0 \mid s$ ו $a_n \mid t$.

תרגיל הראו כי x^5-10x^2+1 אי פריק מעל $\mathbb{Q}$.

הערה: ניתן להראות את זה גם בלי משפט גאוס.

קל לראות כי f אינו מתפרק לגורמים לינאריים מעל $\mathbb{Q}$. נניח כי: $x^5-10x^2+1=(x^3+ax^2+bx+c)(x^2+dx+e)$.

אז אחד מהגורמים מתחלק ב x ולכן יש לו שורש רציונלי שהוא גם שורש של f.

נניח כי x^5-10x^2+1 פריק מעל $\mathbb{Q}$. אז קיים שורש רציונלי $\frac{s}{t}$ של f.

לפי הסעיף הקודם $s \mid 1$ ו $t \mid 1$ ולכן $\frac{s}{t} = \pm 1$.

אבל $f(1) \neq 0$ ו $f(-1) \neq 0$ בסתירה.