Egy polinom szorzatra bonthatósága különböző prímek szerinti maradékok felett

Harcos Gergely

2008. november 11.

Műveletek egy prímszám szerinti maradékokban

- p egy prímszám
- $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ a p szerinti lehetséges maradékok halmaza
- Minden egész szám felfogható $\mathbb{F}_p$-beli elemnek és eszerint adjuk össze és szorozzuk a maradékokat.
- Például $\mathbb{F}_7$-ben $6+3=2$ (hiszen $9=2$), illetve $6\cdot 3=4$ (hiszen $18=4$).
- Tudunk kivonni és nemnulla maradékokkal osztani, például $\mathbb{F}_7$-ben $2-5=4$ és $2/5=6$ (valójában $-5=2$ és $1/5=3$).

Polinom szorzatfelbontása a maradékok felett

- $\mathbb{F}_p$-beli együtthatós polinomon egy $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ alakú kifejezést értünk, ahol a_0, a_1, ..., a_{n-1} mind az $\mathbb{F}_p$-ből valók. Ezeket a szokásos módon adjuk és szorozzuk össze, csak a végén az együtthatók maradékát képezzük. Minden $\mathbb{F}_p$-beli együtthatós polinom felbomlik egyértelműen olyan $\mathbb{F}_p$-beli együtthatós polinomok szorzatára, amik tovább már nem bonthatók.

- Például az $f(x) = x^3 - 3x + 1$ polinom mint $\mathbb{F}_{13}$-beli együtthatós polinom nem bomlik fel kisebb fokúak szorzatára (ő maga a felbontás), ellenben mint $\mathbb{F}_{17}$-beli együtthatós polinom felbomlik elsőfokúak szorzatára:

$$x^3 - 3x + 1 = (x-7)(x-13)(x-14).$$

A számelmélet egy izgalmas és mély kérdése

- $f(x)$ egy rögzített egész együtthatós polinom
- p végigfut a prímeken egy nagy korlátig
- Az $f(x)$-et a különféle $\mathbb{F}_p$-beli együtthatós polinomok körében felbontva a keletkező tényezők fokszámai követnek-e valamilyen statisztikát, esetleg szabályos mintát a p-ben?
- Megnézünk néhány példát: x^2-2, x^2-3x+1, x^3-2, x^3-3x+1, x^4-x^2-1, x^4-x-1.

In[59]:=
```
TableForm[Table[{Prime[n], Factor[x^2 - 2, Modulus → Prime[n]]}, {n, 1, 100}]]
```

Out[59]//TableForm=

2	x^2
3	$1 + x^2$
5	$3 + x^2$
7	$(3 + x)\,(4 + x)$
11	$9 + x^2$
13	$11 + x^2$
17	$(6 + x)\,(11 + x)$
19	$17 + x^2$
23	$(5 + x)\,(18 + x)$
29	$27 + x^2$
31	$(8 + x)\,(23 + x)$
37	$35 + x^2$
41	$(17 + x)\,(24 + x)$
43	$41 + x^2$
47	$(7 + x)\,(40 + x)$
53	$51 + x^2$
59	$57 + x^2$
61	$59 + x^2$
67	$65 + x^2$
71	$(12 + x)\,(59 + x)$
73	$(32 + x)\,(41 + x)$
79	$(9 + x)\,(70 + x)$
83	$81 + x^2$
89	$(25 + x)\,(64 + x)$
97	$(14 + x)\,(83 + x)$
101	$99 + x^2$
103	$(38 + x)\,(65 + x)$
107	$105 + x^2$
109	$107 + x^2$
113	$(51 + x)\,(62 + x)$
127	$(16 + x)\,(111 + x)$
131	$129 + x^2$
137	$(31 + x)\,(106 + x)$
139	$137 + x^2$
149	$147 + x^2$
151	$(46 + x)\,(105 + x)$
157	$155 + x^2$
163	$161 + x^2$
167	$(13 + x)\,(154 + x)$
173	$171 + x^2$
179	$177 + x^2$
181	$179 + x^2$
191	$(57 + x)\,(134 + x)$
193	$(52 + x)\,(141 + x)$
197	$195 + x^2$
199	$(20 + x)\,(179 + x)$
211	$209 + x^2$
223	$(15 + x)\,(208 + x)$
227	$225 + x^2$

In[60]:=
```
TableForm[
 Table[{Prime[n], Mod[Prime[n], 8], Factor[x^2 - 2, Modulus → Prime[n]]}, {n, 1, 100}]]
```

Out[60]//TableForm=

2	2	x^2
3	3	$1 + x^2$
5	5	$3 + x^2$
7	7	$(3 + x)\ (4 + x)$
11	3	$9 + x^2$
13	5	$11 + x^2$
17	1	$(6 + x)\ (11 + x)$
19	3	$17 + x^2$
23	7	$(5 + x)\ (18 + x)$
29	5	$27 + x^2$
31	7	$(8 + x)\ (23 + x)$
37	5	$35 + x^2$
41	1	$(17 + x)\ (24 + x)$
43	3	$41 + x^2$
47	7	$(7 + x)\ (40 + x)$
53	5	$51 + x^2$
59	3	$57 + x^2$
61	5	$59 + x^2$
67	3	$65 + x^2$
71	7	$(12 + x)\ (59 + x)$
73	1	$(32 + x)\ (41 + x)$
79	7	$(9 + x)\ (70 + x)$
83	3	$81 + x^2$
89	1	$(25 + x)\ (64 + x)$
97	1	$(14 + x)\ (83 + x)$
101	5	$99 + x^2$
103	7	$(38 + x)\ (65 + x)$
107	3	$105 + x^2$
109	5	$107 + x^2$
113	1	$(51 + x)\ (62 + x)$
127	7	$(16 + x)\ (111 + x)$
131	3	$129 + x^2$
137	1	$(31 + x)\ (106 + x)$
139	3	$137 + x^2$
149	5	$147 + x^2$
151	7	$(46 + x)\ (105 + x)$
157	5	$155 + x^2$
163	3	$161 + x^2$
167	7	$(13 + x)\ (154 + x)$
173	5	$171 + x^2$
179	3	$177 + x^2$
181	5	$179 + x^2$
191	7	$(57 + x)\ (134 + x)$
193	1	$(52 + x)\ (141 + x)$
197	5	$195 + x^2$
199	7	$(20 + x)\ (179 + x)$
211	3	$209 + x^2$
223	7	$(15 + x)\ (208 + x)$

In[61]:=
```
TableForm[Table[{Prime[n], Factor[x^2 - 3 x + 1, Modulus → Prime[n]]}, {n, 1, 100}]]
```

Out[61]//TableForm=

2	$1 + x + x^2$
3	$1 + x^2$
5	$(1 + x)^2$
7	$1 + 4\,x + x^2$
11	$(2 + x)\,(6 + x)$
13	$1 + 10\,x + x^2$
17	$1 + 14\,x + x^2$
19	$(3 + x)\,(13 + x)$
23	$1 + 20\,x + x^2$
29	$(4 + x)\,(22 + x)$
31	$(11 + x)\,(17 + x)$
37	$1 + 34\,x + x^2$
41	$(5 + x)\,(33 + x)$
43	$1 + 40\,x + x^2$
47	$1 + 44\,x + x^2$
53	$1 + 50\,x + x^2$
59	$(24 + x)\,(32 + x)$
61	$(16 + x)\,(42 + x)$
67	$1 + 64\,x + x^2$
71	$(7 + x)\,(61 + x)$
73	$1 + 70\,x + x^2$
79	$(28 + x)\,(48 + x)$
83	$1 + 80\,x + x^2$
89	$(8 + x)\,(78 + x)$
97	$1 + 94\,x + x^2$
101	$(21 + x)\,(77 + x)$
103	$1 + 100\,x + x^2$
107	$1 + 104\,x + x^2$
109	$(9 + x)\,(97 + x)$
113	$1 + 110\,x + x^2$
127	$1 + 124\,x + x^2$
131	$(10 + x)\,(118 + x)$
137	$1 + 134\,x + x^2$
139	$(62 + x)\,(74 + x)$
149	$(39 + x)\,(107 + x)$
151	$(26 + x)\,(122 + x)$
157	$1 + 154\,x + x^2$
163	$1 + 160\,x + x^2$
167	$1 + 164\,x + x^2$
173	$1 + 170\,x + x^2$
179	$(73 + x)\,(103 + x)$
181	$(12 + x)\,(166 + x)$
191	$(87 + x)\,(101 + x)$
193	$1 + 190\,x + x^2$
197	$1 + 194\,x + x^2$
199	$(60 + x)\,(136 + x)$
211	$(31 + x)\,(177 + x)$
223	$1 + 220\,x + x^2$
227	$1 + 224\,x + x^2$

In[62]:=
```
TableForm[Table[
  {Prime[n], Mod[Prime[n], 20], Factor[x^2 - 3 x + 1, Modulus → Prime[n]]}, {n, 1, 100}]]
```

Out[62]//TableForm=

2	2	$1 + x + x^2$
3	3	$1 + x^2$
5	5	$(1 + x)^2$
7	7	$1 + 4\,x + x^2$
11	11	$(2 + x)\,(6 + x)$
13	13	$1 + 10\,x + x^2$
17	17	$1 + 14\,x + x^2$
19	19	$(3 + x)\,(13 + x)$
23	3	$1 + 20\,x + x^2$
29	9	$(4 + x)\,(22 + x)$
31	11	$(11 + x)\,(17 + x)$
37	17	$1 + 34\,x + x^2$
41	1	$(5 + x)\,(33 + x)$
43	3	$1 + 40\,x + x^2$
47	7	$1 + 44\,x + x^2$
53	13	$1 + 50\,x + x^2$
59	19	$(24 + x)\,(32 + x)$
61	1	$(16 + x)\,(42 + x)$
67	7	$1 + 64\,x + x^2$
71	11	$(7 + x)\,(61 + x)$
73	13	$1 + 70\,x + x^2$
79	19	$(28 + x)\,(48 + x)$
83	3	$1 + 80\,x + x^2$
89	9	$(8 + x)\,(78 + x)$
97	17	$1 + 94\,x + x^2$
101	1	$(21 + x)\,(77 + x)$
103	3	$1 + 100\,x + x^2$
107	7	$1 + 104\,x + x^2$
109	9	$(9 + x)\,(97 + x)$
113	13	$1 + 110\,x + x^2$
127	7	$1 + 124\,x + x^2$
131	11	$(10 + x)\,(118 + x)$
137	17	$1 + 134\,x + x^2$
139	19	$(62 + x)\,(74 + x)$
149	9	$(39 + x)\,(107 + x)$
151	11	$(26 + x)\,(122 + x)$
157	17	$1 + 154\,x + x^2$
163	3	$1 + 160\,x + x^2$
167	7	$1 + 164\,x + x^2$
173	13	$1 + 170\,x + x^2$
179	19	$(73 + x)\,(103 + x)$
181	1	$(12 + x)\,(166 + x)$
191	11	$(87 + x)\,(101 + x)$
193	13	$1 + 190\,x + x^2$
197	17	$1 + 194\,x + x^2$
199	19	$(60 + x)\,(136 + x)$
211	11	$(31 + x)\,(177 + x)$
223	3	$1 + 220\,x + x^2$

A másodfokú példák összefoglalása

- x^2-2 az esetek felében (amikor p maradéka 8-cal osztva $3,5$) felbonthatatlan, a másik felében (amikor p maradéka 8-cal osztva $1,7$) két elsőfokú polinom szorzata.

- x^2-3x+1 az esetek felében (amikor p maradéka 20-szal osztva $3,7,13,17$) felbonthatatlan, a másik felében (amikor p maradéka 20-szal osztva $1,9,11,19$) két elsőfokú polinom szorzata.

- Általában igaz, hogy x^2+ax+b az esetek felében felbonthatatlan, a másik felében két elsőfokú szorzata. Hogy melyik eset áll fenn, az csakis a p-nek a $[4,a^2-4b]$ számmal vett maradékától függ.

In[69]:=
```
TableForm[Table[{Prime[n], Factor[x^3 - 2, Modulus → Prime[n]]}, {n, 1, 100}]]
```

Out[69]//TableForm=

2	x^3
3	$(1 + x)^3$
5	$(2 + x)\,(4 + 3\,x + x^2)$
7	$5 + x^3$
11	$(4 + x)\,(5 + 7\,x + x^2)$
13	$11 + x^3$
17	$(9 + x)\,(13 + 8\,x + x^2)$
19	$17 + x^3$
23	$(7 + x)\,(3 + 16\,x + x^2)$
29	$(3 + x)\,(9 + 26\,x + x^2)$
31	$(11 + x)\,(24 + x)\,(27 + x)$
37	$35 + x^3$
41	$(36 + x)\,(25 + 5\,x + x^2)$
43	$(9 + x)\,(11 + x)\,(23 + x)$
47	$(26 + x)\,(18 + 21\,x + x^2)$
53	$(35 + x)\,(6 + 18\,x + x^2)$
59	$(21 + x)\,(28 + 38\,x + x^2)$
61	$59 + x^3$
67	$65 + x^3$
71	$(22 + x)\,(58 + 49\,x + x^2)$
73	$71 + x^3$
79	$77 + x^3$
83	$(33 + x)\,(10 + 50\,x + x^2)$
89	$(73 + x)\,(78 + 16\,x + x^2)$
97	$95 + x^3$
101	$(75 + x)\,(70 + 26\,x + x^2)$
103	$101 + x^3$
107	$(101 + x)\,(36 + 6\,x + x^2)$
109	$(6 + x)\,(51 + x)\,(52 + x)$
113	$(32 + x)\,(7 + 81\,x + x^2)$
127	$(5 + x)\,(27 + x)\,(95 + x)$
131	$(77 + x)\,(34 + 54\,x + x^2)$
137	$(39 + x)\,(14 + 98\,x + x^2)$
139	$137 + x^3$
149	$(79 + x)\,(132 + 70\,x + x^2)$
151	$149 + x^3$
157	$(21 + x)\,(41 + x)\,(95 + x)$
163	$161 + x^3$
167	$(10 + x)\,(100 + 157\,x + x^2)$
173	$(12 + x)\,(144 + 161\,x + x^2)$
179	$(121 + x)\,(142 + 58\,x + x^2)$
181	$179 + x^3$
191	$(44 + x)\,(26 + 147\,x + x^2)$
193	$191 + x^3$
197	$(176 + x)\,(47 + 21\,x + x^2)$
199	$197 + x^3$
211	$209 + x^3$
223	$(24 + x)\,(44 + x)\,(155 + x)$

```
In[70]:= TableForm[Table[{Prime[n], Factor[x^3 - 3 x + 1, Modulus → Prime[n]]}, {n, 1, 100}]]
```

Out[70]//TableForm=

2	$1 + x + x^3$
3	$(1 + x)^3$
5	$1 + 2x + x^3$
7	$1 + 4x + x^3$
11	$1 + 8x + x^3$
13	$1 + 10x + x^3$
17	$(3 + x)(4 + x)(10 + x)$
19	$(10 + x)(12 + x)(16 + x)$
23	$1 + 20x + x^3$
29	$1 + 26x + x^3$
31	$1 + 28x + x^3$
37	$(14 + x)(28 + x)(32 + x)$
41	$1 + 38x + x^3$
43	$1 + 40x + x^3$
47	$1 + 44x + x^3$
53	$(18 + x)(39 + x)(49 + x)$
59	$1 + 56x + x^3$
61	$1 + 58x + x^3$
67	$1 + 64x + x^3$
71	$(16 + x)(25 + x)(30 + x)$
73	$(14 + x)(25 + x)(34 + x)$
79	$1 + 76x + x^3$
83	$1 + 80x + x^3$
89	$(12 + x)(36 + x)(41 + x)$
97	$1 + 94x + x^3$
101	$1 + 98x + x^3$
103	$1 + 100x + x^3$
107	$(7 + x)(40 + x)(60 + x)$
109	$(5 + x)(18 + x)(86 + x)$
113	$1 + 110x + x^3$
127	$(53 + x)(87 + x)(114 + x)$
131	$1 + 128x + x^3$
137	$1 + 134x + x^3$
139	$1 + 136x + x^3$
149	$1 + 146x + x^3$
151	$1 + 148x + x^3$
157	$1 + 154x + x^3$
163	$(70 + x)(101 + x)(155 + x)$
167	$1 + 164x + x^3$
173	$1 + 170x + x^3$
179	$(34 + x)(46 + x)(99 + x)$
181	$(46 + x)(58 + x)(77 + x)$
191	$1 + 188x + x^3$
193	$1 + 190x + x^3$
197	$(6 + x)(28 + x)(163 + x)$
199	$(40 + x)(165 + x)(193 + x)$
211	$1 + 208x + x^3$
223	$1 + 220x + x^3$
227	$1 + 224x + x^3$

```
In[71]:= TableForm[Table[
           {Prime[n], Mod[Prime[n], 9], Factor[x^3 - 3 x + 1, Modulus → Prime[n]]}, {n, 1, 100}]]
```

Out[71]//TableForm=

2	2	$1 + x + x^3$
3	3	$(1 + x)^3$
5	5	$1 + 2\,x + x^3$
7	7	$1 + 4\,x + x^3$
11	2	$1 + 8\,x + x^3$
13	4	$1 + 10\,x + x^3$
17	8	$(3 + x)\,(4 + x)\,(10 + x)$
19	1	$(10 + x)\,(12 + x)\,(16 + x)$
23	5	$1 + 20\,x + x^3$
29	2	$1 + 26\,x + x^3$
31	4	$1 + 28\,x + x^3$
37	1	$(14 + x)\,(28 + x)\,(32 + x)$
41	5	$1 + 38\,x + x^3$
43	7	$1 + 40\,x + x^3$
47	2	$1 + 44\,x + x^3$
53	8	$(18 + x)\,(39 + x)\,(49 + x)$
59	5	$1 + 56\,x + x^3$
61	7	$1 + 58\,x + x^3$
67	4	$1 + 64\,x + x^3$
71	8	$(16 + x)\,(25 + x)\,(30 + x)$
73	1	$(14 + x)\,(25 + x)\,(34 + x)$
79	7	$1 + 76\,x + x^3$
83	2	$1 + 80\,x + x^3$
89	8	$(12 + x)\,(36 + x)\,(41 + x)$
97	7	$1 + 94\,x + x^3$
101	2	$1 + 98\,x + x^3$
103	4	$1 + 100\,x + x^3$
107	8	$(7 + x)\,(40 + x)\,(60 + x)$
109	1	$(5 + x)\,(18 + x)\,(86 + x)$
113	5	$1 + 110\,x + x^3$
127	1	$(53 + x)\,(87 + x)\,(114 + x)$
131	5	$1 + 128\,x + x^3$
137	2	$1 + 134\,x + x^3$
139	4	$1 + 136\,x + x^3$
149	5	$1 + 146\,x + x^3$
151	7	$1 + 148\,x + x^3$
157	4	$1 + 154\,x + x^3$
163	1	$(70 + x)\,(101 + x)\,(155 + x)$
167	5	$1 + 164\,x + x^3$
173	2	$1 + 170\,x + x^3$
179	8	$(34 + x)\,(46 + x)\,(99 + x)$
181	1	$(46 + x)\,(58 + x)\,(77 + x)$
191	2	$1 + 188\,x + x^3$
193	4	$1 + 190\,x + x^3$
197	8	$(6 + x)\,(28 + x)\,(163 + x)$
199	1	$(40 + x)\,(165 + x)\,(193 + x)$
211	4	$1 + 208\,x + x^3$
223	7	$1 + 220\,x + x^3$

A harmadfokú példák összefoglalása

- x^3-2 az esetek harmadában felbonthatatlan, az esetek felében egy elsőfokú és egy másodfokú felbonthatatlan polinom szorzata, és az esetek egyhatodában három elsőfokú polinom szorzata.

- x^3-3x+1 az esetek kétharmadában (amikor $p \equiv 2,4,5,7 \pmod 9$) felbonthatatlan, az esetek harmadában (amikor $p \equiv 1,8 \pmod 9$) pedig három elsőfokú polinom szorzata.

- Általában igaz, hogy x^3+ax^2+bx+c csak a fenti kétféle statisztikát tudja produkálni. A második statisztika akkor és csak akkor fordul elő, ha $-4b^3-27c^2+18abc-4a^3c+a^2b^2$ négyzetszám.

In[78]:=
```
TableForm[Table[{Prime[n], Factor[x^4 - x - 1, Modulus → Prime[n]]}, {n, 1, 100}]]
```

Out[78]//TableForm=

2	$1 + x + x^4$
3	$2 + 2\,x + x^4$
5	$4 + 4\,x + x^4$
7	$(4 + x)\,(5 + 2\,x + 3\,x^2 + x^3)$
11	$(8 + x)\,(4 + 9\,x + 3\,x^2 + x^3)$
13	$(11 + x)\,(7 + 4\,x + 2\,x^2 + x^3)$
17	$(2 + x)\,(5 + x)\,(5 + 10\,x + x^2)$
19	$18 + 18\,x + x^4$
23	$(11 + x)\,(2 + 6\,x + 12\,x^2 + x^3)$
29	$(7 + x)\,(4 + 20\,x + 22\,x^2 + x^3)$
31	$30 + 30\,x + x^4$
37	$(4 + x)\,(5 + x)\,(24 + 28\,x + x^2)$
41	$(19 + x)\,(28 + 33\,x + 22\,x^2 + x^3)$
43	$42 + 42\,x + x^4$
47	$46 + 46\,x + x^4$
53	$(18 + x)\,(41 + x)\,(40 + 47\,x + x^2)$
59	$(32 + x)\,(35 + 21\,x + 27\,x^2 + x^3)$
61	$(53 + x)\,(23 + 3\,x + 8\,x^2 + x^3)$
67	$(21 + x)\,(59 + x)\,(2 + 54\,x + x^2)$
71	$(51 + 15\,x + x^2)\,(32 + 56\,x + x^2)$
73	$(16 + 35\,x + x^2)\,(41 + 38\,x + x^2)$
79	$(15 + x)\,(62 + x)\,(22 + 2\,x + x^2)$
83	$(3 + x)\,(7 + x)\,(14 + x)\,(59 + x)$
89	$(46 + x)\,(29 + 69\,x + 43\,x^2 + x^3)$
97	$(34 + x)\,(77 + 89\,x + 63\,x^2 + x^3)$
101	$(24 + 34\,x + x^2)\,(21 + 67\,x + x^2)$
103	$(85 + x)\,(63 + 15\,x + 18\,x^2 + x^3)$
107	$(64 + x)\,(71 + x)\,(92 + 79\,x + x^2)$
109	$108 + 108\,x + x^4$
113	$(14 + 19\,x + x^2)\,(8 + 94\,x + x^2)$
127	$(93 + 52\,x + x^2)\,(71 + 75\,x + x^2)$
131	$(27 + x)\,(41 + x)\,(111 + 63\,x + x^2)$
137	$(65 + x)\,(59 + 115\,x + 72\,x^2 + x^3)$
139	$138 + 138\,x + x^4$
149	$148 + 148\,x + x^4$
151	$(134 + x)\,(80 + 138\,x + 17\,x^2 + x^3)$
157	$(69 + x)\,(91 + 51\,x + 88\,x^2 + x^3)$
163	$(142 + x)\,(132 + 115\,x + 21\,x^2 + x^3)$
167	$166 + 166\,x + x^4$
173	$172 + 172\,x + x^4$
179	$(123 + x)\,(16 + 93\,x + 56\,x^2 + x^3)$
181	$(24 + 22\,x + x^2)\,(98 + 159\,x + x^2)$
191	$(48 + x)\,(146 + x)\,(68 + 188\,x + x^2)$
193	$(131 + x)\,(139 + x)\,(72 + 116\,x + x^2)$
197	$(84 + x)\,(175 + x)\,(176 + 135\,x + x^2)$
199	$(35 + x)\,(108 + 31\,x + 164\,x^2 + x^3)$
211	$(30 + x)\,(7 + 56\,x + 181\,x^2 + x^3)$
223	$222 + 222\,x + x^4$

```
In[79]:= TableForm[Table[{Prime[n], Factor[x^4 - x^2 - 1, Modulus → Prime[n]]}, {n, 1, 100}]]
```

Out[79]//TableForm=

2	$(1 + x + x^2)^2$
3	$2 + 2\,x^2 + x^4$
5	$(2 + x^2)^2$
7	$6 + 6\,x^2 + x^4$
11	$(2 + x)\,(9 + x)\,(3 + x^2)$
13	$(8 + 2\,x + x^2)\,(8 + 11\,x + x^2)$
17	$(4 + 3\,x + x^2)\,(4 + 14\,x + x^2)$
19	$(9 + x)\,(10 + x)\,(4 + x^2)$
23	$22 + 22\,x^2 + x^4$
29	$(8 + x)\,(13 + x)\,(16 + x)\,(21 + x)$
31	$(9 + x)\,(22 + x)\,(18 + x^2)$
37	$(31 + 10\,x + x^2)\,(31 + 27\,x + x^2)$
41	$(6 + x^2)\,(34 + x^2)$
43	$42 + 42\,x^2 + x^4$
47	$46 + 46\,x^2 + x^4$
53	$(23 + 10\,x + x^2)\,(23 + 43\,x + x^2)$
59	$(12 + x)\,(47 + x)\,(25 + x^2)$
61	$(17 + x^2)\,(43 + x^2)$
67	$66 + 66\,x^2 + x^4$
71	$(3 + x)\,(68 + x)\,(8 + x^2)$
73	$(27 + 36\,x + x^2)\,(27 + 37\,x + x^2)$
79	$(34 + x)\,(45 + x)\,(49 + x^2)$
83	$82 + 82\,x^2 + x^4$
89	$(13 + x)\,(30 + x)\,(59 + x)\,(76 + x)$
97	$(75 + 32\,x + x^2)\,(75 + 65\,x + x^2)$
101	$(15 + x)\,(33 + x)\,(68 + x)\,(86 + x)$
103	$102 + 102\,x^2 + x^4$
107	$106 + 106\,x^2 + x^4$
109	$(10 + x^2)\,(98 + x^2)$
113	$(15 + 12\,x + x^2)\,(15 + 101\,x + x^2)$
127	$126 + 126\,x^2 + x^4$
131	$(55 + x)\,(76 + x)\,(11 + x^2)$
137	$(100 + 8\,x + x^2)\,(100 + 129\,x + x^2)$
139	$(8 + x)\,(131 + x)\,(63 + x^2)$
149	$(40 + x^2)\,(108 + x^2)$
151	$(44 + x)\,(107 + x)\,(123 + x^2)$
157	$(28 + 34\,x + x^2)\,(28 + 123\,x + x^2)$
163	$162 + 162\,x^2 + x^4$
167	$166 + 166\,x^2 + x^4$
173	$(93 + 35\,x + x^2)\,(93 + 138\,x + x^2)$
179	$(84 + x)\,(95 + x)\,(74 + x^2)$
181	$(63 + x)\,(75 + x)\,(106 + x)\,(118 + x)$
191	$(26 + x)\,(165 + x)\,(102 + x^2)$
193	$(112 + 15\,x + x^2)\,(112 + 178\,x + x^2)$
197	$(14 + 63\,x + x^2)\,(14 + 134\,x + x^2)$
199	$(96 + x)\,(103 + x)\,(61 + x^2)$
211	$(50 + x)\,(161 + x)\,(178 + x^2)$
223	$222 + 222\,x^2 + x^4$

A negyedfokú példák összefoglalása

- $x^4 - x - 1$ az esetek $1/4$ részében felbonthatatlan, $1/3$ részében egy elsőfokú és egy harmadfokú felbonthatatlan polinom szorzata, $1/8$ részében két másodfokú felbonthatatlan polinom szorzata, $1/4$ részében két elsőfokú és egy másodfokú felbonthatatlan polinom szorzata, $1/24$ részében pedig négy elsőfokú polinom szorzata.

- $x^4 - x^2 - 1$ az esetek $1/4$ részében felbonthatatlan, $3/8$ részében két másodfokú felbonthatatlan polinom szorzata, az esetek $1/4$ részében két elsőfokú és egy másodfokú felbonthatatlan polinom szorzata, az esetek $1/8$ részében pedig négy elsőfokú polinom szorzata.

Galois és Csebotarejev tételei

Legyen n rögzített pozitív egész, $f(x)$ pedig az egészek fölött felbonthatatlan n-edfokú polinom. A különböző prímek szerinti fokszám-statisztikában minden sűrűség egy $n!$ nevezőjű törtszám. Az $f(x)$ szimmetriacsoportja határozza meg a sűrűségeket. Ha a szimmetriacsoport a lehető legnagyobb, akkor mindegyik lehetséges fokszám-kombináció előfordul pozitív sűrűséggel és a csupa elsőfokú tényezőre bomlás sűrűsége $1/n!$. Minden más esetben a csupa elsőfokú tényezőre bomlás sűrűsége $1/n!$-nál nagyobb.

Langlands sejtései

A legtöbb $f(x)$-re nincs egyszerű maradékos jellemzése az egyes fokszám-kombinációkat szolgáltató prímeknek. Mindazonáltal úgy sejtjük, hogy ezek valamilyen általánosított értelemben mégis periodikusak. A precíz megfogalmazáshoz mélyebb matematikai fogalmakat (az ún. automorf formákat) kell segítségül hívnunk, a bizonyítástól pedig egyelőre igen távol állunk.