ВХОД: $poly$ - многочлен над полем Галуа $GF[P]$
РЕЗУЛЬТАТ: $true$ если многочлен неприводим, иначе $false$

1: if $poly = 0$ then
2: return $false$
3: end if
4: $n = deg(poly)$
5: if $n = 0$ or ($poly[0] = 0$ and $n > 1$) then
6: return $false$
7: end if
8: if $n = 1$ then
9: return $true$
10: end if
11:
12: $poly' = \frac{\partial poly}{\partial x}$
13: if $poly' = 0$ then
14: return $false$
15: end if
16: if $deg\,(gcd\,(poly, poly')) = 0$ then
17: return $false$
18: end if
19: $B = \begin{pmatrix} x^0 & mod & poly \\ x^P & mod & poly \\ \dots & \dots & \dots \\ x^{P\times(P-1)} & mod & poly \end{pmatrix}$
20: $B = B - E$
21: $r = rank(B)$
22: if $r = deg(poly) - 1$ then
23: return $true$
24: else
25: return $false$
26: end if

ВХОД: $poly$ - многочлен над полем Галуа $GF[P]$ степени n,
$p_1, ..., p_k$ – простые делители n
РЕЗУЛЬТАТ: $true$ если многочлен неприводим, иначе $false$

1: if $poly = 0$ then
2: return $false$
3: end if
4: if $n = 0$ or ($poly[0] = 0$ and $n > 1$) then
5: return $false$
6: end if
7: if $n = 1$ then
8: return $true$
9: end if
10:
11: for $i = 1..k$ do
12: $n_i = \frac{n}{p_j}$
13: $g = gcd\left(poly, x^{P^{n_i}} - x \ (mod\ poly)\right)$
14: if $g = 0$ or $deg(g) > 0$ then
15: return $false$
16: end if
17: end for
18: $g = gcd\left(poly, x^{P^n} - x \ (mod\ poly)\right)$
19: if $g = 0$ then
20: return $true$
21: else
22: return $false$
23: end if

ВХОД: $poly$ - многочлен над полем Галуа $GF[P]$
РЕЗУЛЬТАТ: $true$ если многочлен неприводим, иначе $false$

1: if $poly = 0$ then
2: return $false$
3: end if
4: $n = deg(poly)$
5: if $n = 0$ or ($poly[0] = 0$ and $n > 1$) then
6: return $false$
7: end if
8: if $n = 1$ then
9: return $true$
10: end if
11:
12: $n = deg(poly)$
13: for $i = 1..\left[\frac{m}{2}\right]$ do
14: $g = gcd\left(poly, x^{P^i} - x \ (mod\ poly)\right)$
15: if $g = 0$ or $deg(g) > 0$ then
16: return $false$
17: end if
18: end for
19: return $true$

ВХОД: $poly$ - многочлен над полем Галуа $GF[P]$,
$p_1, ..., p_k$ – простые дилители $P-1$ за исключением 1 и самого $P-1$
РЕЗУЛЬТАТ: $true$ если многочлен неприводим, иначе $false$

1: if $poly = 0$ then
2: return $false$
3: end if
4: $n = deg(poly)$
5: if $n = 0$ or ($poly[0] = 0$ and $n > 1$) then
6: return $false$
7: end if
8:
9: $poly = noramlize(poly)$
10: if $poly = x$ then
11: return $true$
12: end if
13: if $P = 2$ and $poly = 1 + x$ then
14: return $false$
15: end if
16:
17: if $P > 2$ then
18: for $i = 1..k$ do
19: $l = (-1)^n \ (mod\ P)$
20: $el = l^{\frac{P-1}{p_i}}$
21: if $el = 1$ then
22: return $false$
23: end if
24: end for
25: end if
26:
27: $l = (-1)^n \ (mod\ P)$
28: $r = \frac{p^n-1}{p-1}$
29: if $x^r \neq l$ then
30: return $false$
31: end if
32:
33: for $i = 1..k$ do
34: $tmp = x^{\frac{r}{q_i}} \ (mod\ poly)$
35: if $deg(tmp) = 0$ then
36: return $false$
37: end if
38: end for
39: return $true$