How Are Irreducible and Primitive Polynomials Distributed over Finite Fields?

Gary L. Mullen

Penn State University

mullen@math.psu.edu

July 21, 2010

Let $q = p^m$ be a prime power

Let $F_q = F_{p^m}$ denote the finite field of order q

Primitive Polynomials

$f \in F_q[x]$ of deg. n is primitive if every root of f is a prim. ele. in F_{q^n}

Recall that a prim. ele. in F_{q^n} generates the mul. group $F_{q^n}^*$

Theorem

Cohen *(Disc. Math., 90) Let* $n \geq 2$ *and let* $a \in F_q$ *(with* $a \neq 0$ *if* $n = 2$ *or if* $n = 3$ *and* $q = 4$*). Then there exists prim. deg.* n *over* F_q *with trace* a*.*

Theorem

Cohen *(Disc. Math., 90) Let* $n \geq 2$ *and let* $a \in F_q$ *(with* $a \neq 0$ *if* $n = 2$ *or if* $n = 3$ *and* $q = 4$*). Then there exists prim. deg.* n *over* F_q *with trace* a*.*

Conjecture

Hansen/M *(Math. Comp, 92)*
Conj A: *For* $n \geq 2$, $0 \leq j < n$ *and given* $a \in F_q$, *there is prim.*
$x^n + \cdots + ax^j + \cdots$ *except when*
(P1) q *arb.,* $j = 0$, $a \neq (-1)^n \alpha$,
α *prim. in* F_q
(P2) q *arb.,* $n = 2, j = 1, a = 0$
(P3) $q = 4, n = 3, j = 2, a = 0$
(P4) $q = 4, n = 3, j = 1, a = 0$
(P5) $q = 2, n = 4, j = 2, a = 1$

Many papers by various people culminating in

Theorem

Cohen *(FFA 06) Conj. A is true for deg.* $n \geq 9$.

Many papers by various people culminating in

Theorem

Cohen *(FFA 06) Conj. A is true for deg.* $n \geq 9$.

Theorem

Cohen/Presern *(Lond. Math. Soc. Lect. Note Ser. 07) Conj. A is true!!*

Other Related Results

Theorem

Han *(Math. Comp., 96) For* q *odd and* $n \geq 7$, $\exists$ *prim. deg.* n *with coeffs. of* x^{n-1} *and* x^{n-2} *given in advance.*

Other Related Results

Theorem

Han *(Math. Comp., 96) For q odd and $n \geq 7$, $\exists$ prim. deg. n with coeffs. of x^{n-1} and x^{n-2} given in advance.*

Theorem

Han *(FFA 97) For q even and $n \geq 7$, $\exists$ prim. deg. n with coeff. x^{n-1} and x^{n-2} given in advance.*

Other Related Results

Theorem

Han *(Math. Comp., 96) For* q *odd and* $n \geq 7$, $\exists$ *prim. deg.* n *with coeffs. of* x^{n-1} *and* x^{n-2} *given in advance.*

Theorem

Han *(FFA 97) For* q *even and* $n \geq 7$, $\exists$ *prim. deg.* n *with coeff.* x^{n-1} *and* x^{n-2} *given in advance.*

Theorem

Cohen/Mills *(FFA 03) For* q *odd and* $n = 5, 6$ $\exists$ *prim. deg.* n *with coeff.* x^{n-1} *and* x^{n-2} *given in advance.*

Other Related Results

Theorem

Han *(Math. Comp., 96) For* q *odd and* $n \geq 7$, $\exists$ *prim. deg.* n *with coeffs. of* x^{n-1} *and* x^{n-2} *given in advance.*

Theorem

Han *(FFA 97) For* q *even and* $n \geq 7$, $\exists$ *prim. deg.* n *with coeff.* x^{n-1} *and* x^{n-2} *given in advance.*

Theorem

Cohen/Mills *(FFA 03) For* q *odd and* $n = 5, 6$ $\exists$ *prim. deg.* n *with coeff.* x^{n-1} *and* x^{n-2} *given in advance.*

Theorem

Shuqin/Han *(FFA 04) For* $n \geq 8$ $\exists$ *prim. deg.* n *with highest three coeff. given in advance.*

Problem

Find formulas, or good estimates, for the # of prim. deg. n *over* F_q *with given trace, (or even more coeff). specified in advance.*

Problem

Find formulas, or good estimates, for the # of prim. deg. n over F_q with given trace, (or even more coeff). specified in advance.

Theorem

Chang/Chou/Shiue *(FFA 05) Enum. results.*

Primitive Normal Polynomials

For $\alpha \in F_{q^n}$, if $A = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a basis over F_q, A is normal basis.

If $\langle \alpha \rangle = F_{q^n}^*$, A is prim. nor. basis.

Theorem

Carlitz *(Trans. 52) Prim. nor. basis over F_p for suff. large p.*

Theorem

Carlitz *(Trans. 52) Prim. nor. basis over F_p for suff. large p.*

Theorem

Davenport *(J. Lond. M. S. 68) Prim. nor. basis over F_p for any prime p.*

Theorem

Carlitz *(Trans. 52) Prim. nor. basis over* F_p *for suff. large* p.

Theorem

Davenport *(J. Lond. M. S. 68) Prim. nor. basis over* F_p *for any prime* p.

Theorem

Lenstra-Schoof *(Math. Comp., 87)* F_{q^n} *has prim. nor. basis over* F_q.

Theorem

Carlitz *(Trans. 52) Prim. nor. basis over* F_p *for suff. large* p.

Theorem

Davenport *(J. Lond. M. S. 68) Prim. nor. basis over* F_p *for any prime* p.

Theorem

Lenstra-Schoof *(Math. Comp., 87)* F_{q^n} *has prim. nor. basis over* F_q.

Theorem

Cohen/Huczynska *(J. London. M. Soc. 03) Prim. nor. basis without a computer!*

$\phi(q^n - 1)$ is # of prim. elem. in F_{q^n}

$\Phi_q(x^n - 1)$ is # of nor. basis elem. in F_{q^n}.

Problem

Find a formula for the number $PN_q(n)$ of prim. nor. elem. in F_{q^n}.

Conjecture

Morgan/Mul. *(Math. Comp., 94) For* $n \geq 2$ *and* $a \in F_q^*$*, there is a prim. nor. poly. deg.* n *over* F_q *with trace* a*.*

True for:

$q = 2$ any n

$n = 2$ any q

$(q-1)|n$

$n \leq 6, q \leq 97$

Theorem

Cohen/Hac. *(AAECC, 99) Morgan/M Conj. true*

Theorem

Cohen/Hac. *(AAECC, 99) Morgan/M Conj. true*

Conjecture

Morgan/Mul. Conj: *(Math. Comp., 94) For p prime and $n \geq 2$, $\exists$ prim. nor. poly. deg. n over F_p with at most 5 nonzero coeffs.*

Theorem

Cohen/Hac. *(AAECC, 99) Morgan/M Conj. true*

Conjecture

Morgan/Mul. Conj: *(Math. Comp., 94) For* p *prime and* $n \geq 2$, $\exists$ *prim. nor. poly. deg.* n *over* F_p *with at most 5 nonzero coeffs.*

Theorem

Cohen *(Pub. Math. Deb. 00) Prim. nor. of deg.* $n \geq 5$ *with given norm and trace.*

Theorem

Cohen/Hac. *(AAECC, 99) Morgan/M Conj. true*

Conjecture

Morgan/Mul. Conj: *(Math. Comp., 94) For* p *prime and* $n \geq 2$, $\exists$ *prim. nor. poly. deg.* n *over* F_p *with at most 5 nonzero coeffs.*

Theorem

Cohen *(Pub. Math. Deb. 00) Prim. nor. of deg.* $n \geq 5$ *with given norm and trace.*

Theorem

Cohen/Huczynska *(Acta Arith, 03) Prim. nor. quartics with given norm and trace*

Theorem

Cohen/Hac. *(AAECC, 99) Morgan/M Conj. true*

Conjecture

Morgan/Mul. Conj: *(Math. Comp., 94) For* p *prime and* $n \geq 2$, $\exists$ *prim. nor. poly. deg.* n *over* F_p *with at most 5 nonzero coeffs.*

Theorem

Cohen *(Pub. Math. Deb. 00) Prim. nor. of deg.* $n \geq 5$ *with given norm and trace.*

Theorem

Cohen/Huczynska *(Acta Arith, 03) Prim. nor. quartics with given norm and trace*

Theorem

Huczynska/Cohen *(Trans. A.M.S. 03) Prim. nor. cubics with given norm and trace*

Theorem

Fan/Wang *(FFA 09) If* $n \geq 15, \exists$ *prim. nor. with any coeff. specified in advance*

Completely Normal Bases

$$F_q \subseteq F_{q^d} \subseteq F_{q^n}$$

$\exists \alpha \in F_{q^n}$ nor. basis over F_q and F_{q^d} ?

$\exists \alpha \in F_{q^n}$ nor. basis over F_{q^d} for all $d|n$?

Theorem

Blessenohl/Johnsen *(J. Alg., 86)* F_{q^n} *has a com. nor. basis.*

Conjecture

Morgan/M *(Util. Math. 96) For each $n \geq 2$ there is a com. nor. prim. poly. deg. n over F_q.*

True for: $n = 4$

$q^n \leq 2^{31}, q \leq 97$

Theorem

Shparlinski/Mul. *(Finite Fields Appl., CUP, 96) For $q \geq Cn$log n, $\exists$ com. nor. prim. basis of F_{q^n} over F_q.*

Conjecture

Morgan/M *(Util. Math. 96) For each $n \geq 2$ there is a com. nor. prim. poly. deg. n over F_q.*

True for: $n = 4$

$q^n \leq 2^{31}, q \leq 97$

Theorem

Shparlinski/Mul. *(Finite Fields Appl., CUP, 96) For $q \geq Cn\log n$, $\exists$ com. nor. prim. basis of F_{q^n} over F_q.*

Problem

Find formula for the number $CN_q(n)$ of com. nor. bases of F_{q^n} over F_q.

Irreducibles

Conjecture

Hansen/M *(Math. Comp. 92)*
Conj B: *For* $n \geq 2$, $0 \leq j < n$ *and given* $a \in F_q$ *there is irr.*
$x^n + \cdots + ax^j + \cdots$ *except*
(I1) q *arb.* $j = a = 0$
(I2) $q = 2^m, n = 2, j = 1, a = 0$

Irreducibles

Conjecture

Hansen/M *(Math. Comp. 92)*
Conj B: *For* $n \geq 2$, $0 \leq j < n$ *and given* $a \in F_q$ *there is irr.* $x^n + \cdots + ax^j + \cdots$ *except*
(I1) q *arb.* $j = a = 0$
(I2) $q = 2^m, n = 2, j = 1, a = 0$

Theorem

Wan *(Math. Comp., 97) If either* $q > 19$ *or* $n \geq 36$, *Conj. B is true.*

Irreducibles

Conjecture

Hansen/M *(Math. Comp. 92)*
Conj B: *For* $n \geq 2$, $0 \leq j < n$ *and given* $a \in F_q$ *there is irr.*
$x^n + \cdots + ax^j + \cdots$ *except*
(I1) q *arb.* $j = a = 0$
(I2) $q = 2^m, n = 2, j = 1, a = 0$

Theorem

Wan *(Math. Comp., 97) If either* $q > 19$ *or* $n \geq 36$, *Conj. B is true.*

Theorem

Ham/Mul. *(Math. Comp. 97) Conj. B is true.*

Theorem

Hsu *(J. Numb. Thy., 96) (i) If* f *has even deg.* n *and* $q \geq n/2+1$, $\exists$ *irr.* P *of deg.* n *with deg.* $(P-f)$ *at most* $n/2$.
(ii) If f *has odd deg.* n *and* $q \geq ((n+3)/2)^2$, $\exists$ *irr.* P *of deg.* n *with deg.* $(P-f)$ *at most* $(n-1)/2$.

Exact Formulas

$N_q(n) = \#$ monic irr. deg. n

$$= \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}$$

$\#$ monic irr. deg. n trace 1

$$\frac{1}{2n} \sum_{d|n, d odd} \mu(d) 2^{n/d}$$

Fix $1 \leq j \leq n, \beta \in F_{2^n}$

$$T_j(\beta) = \sum_{0 \leq i_1 < i_2 < \cdots < i_j \leq n} \beta^{2^{i_1}} \beta^{2^{i_2}} \cdots \beta^{2^{i_j}}$$

$T_j : F_{2^n} \rightarrow F_2$

$T_1(\beta) = \beta + \beta^2 + \beta^{2^2} + \cdots + \beta^{2^{n-1}}$

$F(n, t_1, \ldots, t_r) = \#\beta \in F_{2^n}$ with $T_j(\beta) = t_j, j = 1, \ldots, r$

$P(n, t_1, \ldots, t_r) = \#$ irr. deg n with coeff. $x^{n-j} = t_j, j = 1, \ldots, r$

$P(n, 0, 0, 1) = \#x^n + 0x^{n-1} + 0x^{n-2} + 1x^{n-3} + \ldots$

$$nP(n, 0, 0, 1) = \sum_{d|n, dodd} \mu(d) F(n/d, 0, 0, 1)$$

Theorem

Cattell/Miers/Ruskey/Serra/Sawada *(JCMCC 03)*
$F(n, t_1, t_2) = 2^{n-2} + G(n, t_1, t_2)$,

$$G(n,t_1,t_2) = \begin{array}{c|cccc} \underline{m(mod4)} & \underline{00} & \underline{01} & \underline{10} & \underline{11} \\ \underline{0} & -2^{m-1} & 2^{m-1} & 0 & 0 \\ \underline{1} & 0 & 0 & -2^{m-1} & 2^{m-1} \\ \underline{2} & 2^{m-1} & -2^{m-1} & 0 & 0 \\ \underline{3} & 0 & 0 & 2^{m-1} & -2^{m-1} \end{array}$$

Theorem

Kuz'min *(Sov. Math. Dokl. 91)*

Theorem

Yucas/M *(Disc. Math. 04) For* n *even,*
$F(n, t_1, t_2, t_3) = 2^{n-3} + G(n, t_1, t_2, t_3)$,

$\underline{m(mod12)}$	$\underline{000}$	$\underline{001}$	$\underline{010}$	$\underline{011}$
$\underline{0}$	$-2^m - 2^{m-2}$	$2^{m-1} + 2^{m-2}$	2^{m-2}	2^{m-2}
$\underline{1 or 5}$	2^{m-2}	-2^{m-2}	2^{m-2}	-2^{m-2}
$\underline{2 or 10}$	0	2^{m-1}	0	-2^{m-1}
$\underline{3}$	2^{m-2}	-2^{m-2}	2^{m-2}	-2^{m-2}
$\underline{4 or 8}$	-2^{m-1}	0	-2^{m-1}	2^m
$\underline{6}$	$2^{m-1} + 2^{m-2}$	-2^{m-2}	$-2^{m-1} - 2^{m-2}$	2^{m-2}
$\underline{7 or 11}$	2^{m-2}	-2^{m-2}	2^{m-2}	-2^{m-2}
$\underline{9}$	2^{m-2}	-2^{m-2}	2^{m-2}	-2^{m-2}

Theorem

$\underline{m(mod12)}$	$\underline{100}$	$\underline{101}$	$\underline{110}$	$\underline{111}$
$\underline{0}$	0	0	0	0
$\underline{1or5}$	-2^{m-2}	-2^{m-2}	$2^{m-1}+2^{m-2}$	-2^{m-2}
$\underline{2or10}$	2^{m-1}	-2^{m-1}	-2^{m-1}	2^{m-1}
$\underline{3}$	2^{m-1}	0	2^{m-1}	-2^{m}
$\underline{4or8}$	0	0	0	0
$\underline{6}$	2^{m-1}	-2^{m-1}	-2^{m-1}	2^{m-1}
$\underline{7or11}$	-2^{m-2}	$2^{m-1}+2^{m-2}$	-2^{m-2}	-2^{m-2}
$\underline{9}$	-2^{m}	2^{m-1}	0	2^{m-1}

Conjecture

Yucas/Mul *If* $n = 2m$, $F(n, t_1, \ldots, t_r) =$

$$2^{n-r} + a_{m-s+1}2^{m-s+1} + \cdots + a_m 2^m$$

$1 \le s \le m, a_i = -1, 0, 1$

Theorem

Fitzgerald/Yucas *(FFA 03) Formula for* $F(n, t_1, t_2, t_3)$ *for odd* n.
non-deg., alt., sym., bil., quad. forms

Problem

Extend to more than three coeff. over F_2.

Problem

Extend to more than three coeff. over F_2.

Problem

Extend two coeff. case to F_q for $q \geq 2$.

Problem

Extend to more than three coeff. over F_2.

Problem

Extend two coeff. case to F_q *for* $q \geq 2$.

Problem

Extend to j *coeff. over* F_q.

Several Variables

Theorem

Corteel/Savage/Wilf/Zeilberger, (JCT,A 98) The # of pairs of polys. $f(x)$ and $g(x)$ of deg. m over F_2 with $(f,g) = 1$ is the same as the # of pairs of polys. of deg. m with $(f,g) \neq 1$.

Several Variables

Theorem

Corteel/Savage/Wilf/Zeilberger, (JCT,A 98) The # of pairs of polys. $f(x)$ and $g(x)$ of deg. m over F_2 with $(f,g)=1$ is the same as the # of pairs of polys. of deg. m with $(f,g)\neq 1$.

Theorem

Benjamin/Bennett, (Math. Mag. 07), Euclid algor. biject.

Let $f \in F_q[x_1, \ldots, x_k]$ with $k \geq 2$

Two notions: total deg. and vector deg. of f

Problem

Count # of irr. polys. of a given deg. in $F_q[x_1, \ldots, x_k]$

Let $f \in F_q[x_1, \ldots, x_k]$ with $k \geq 2$

Two notions: total deg. and vector deg. of f

Problem

Count # of irr. polys. of a given deg. in $F_q[x_1, \ldots, x_k]$

Problem

Count # of pairs of relatively prime polys. of a given deg. in $F_q[x_1, \ldots, x_k]$

Each problem has a total deg. version and a vector deg. version

Hou/Mul. (FFA 09) Results for several variables

Hou/Mul. (FFA 09) Results for several variables

Bodin (FFA 10) Generating series for # irr. of given deg. and for indecomp. polys.