Modified Conway Polynomials

Frank Lübeck
(Lehrstuhl D für Mathematik, RWTH Aachen)

Sage Days 23, Leiden, July 2010

Compatible Generators of Cyclic Groups

$m \in \mathbb{N}$, C_m: cyclic group of order m

Definition. Let D be a set of divisors of m, closed under gcd. We call $(a_d)_{d \in D}$ a set of compatible generators for D, if each $a_d \in C_m$ has order d and

$$a_d^{d/d'} = a_{d'} \text{ for all } d, d' \in D \text{ with } d' \mid d.$$

Proposition. Assume $m \notin D$ and let $(a_d)_{d \in D}$ be a set of compatible generators for D. Then there exists $a_m \in C_m$ of order m with $a_m^{m/d} = a_d$ for all $d \in D$. If $l = \operatorname{lcm}(D)$ then $a_m^{m/l}$ is uniquely determined by the $(a_d)_{d \in D}$.

Idea of proof. Let c be any generator of C_m and express each $a_d = (c^{m/d})^{r_d}$. With the ansatz $a_m = c^i$ translate the conditions on a_m to congruence equations for i modulo all $d \in D$ and $m/l / \gcd(l, m)$. The compatibility conditions of the a_d ensure that the Chinese remainder theorem yields a solution. A solution can be constructed using the extended Euclidean algorithm.

Compatible Generators of Cyclic Groups

$m \in \mathbb{N}$, C_m: cyclic group of order m

Definition. Let D be a set of divisors of m, closed under gcd. We call $(a_d)_{d\in D}$ a set of compatible generators for D, if each $a_d \in C_m$ has order d and

$$a_d^{d/d'} = a_{d'} \text{ for all } d, d' \in D \text{ with } d' \mid d.$$

Proposition. Assume $m \notin D$ and let $(a_d)_{d\in D}$ be a set of compatible generators for D. Then there exists $a_m \in C_m$ of order m with $a_m^{m/d} = a_d$ for all $d \in D$. If $l = \operatorname{lcm}(D)$ then $a_m^{m/l}$ is uniquely determined by the $(a_d)_{d\in D}$.

Idea of proof. Let c be any generator of C_m and express each $a_d = (c^{m/d})^{r_d}$. With the ansatz $a_m = c^i$ translate the conditions on a_m to congruence equations for i modulo all $d \in D$ and $m/l/\gcd(l, m)$. The compatibility conditions of the a_d ensure that the Chinese remainder theorem yields a solution. A solution can be constructed using the extended Euclidean algorithm.

Compatible Generators of Cyclic Groups

$m \in \mathbb{N}$, C_m: cyclic group of order m

Definition. Let D be a set of divisors of m, closed under gcd. We call $(a_d)_{d\in D}$ a set of compatible generators for D, if each $a_d \in C_m$ has order d and

$$a_d^{d/d'} = a_{d'} \text{ for all } d, d' \in D \text{ with } d' \mid d.$$

Proposition. Assume $m \notin D$ and let $(a_d)_{d\in D}$ be a set of compatible generators for D. Then there exists $a_m \in C_m$ of order m with $a_m^{m/d} = a_d$ for all $d \in D$. If $l = \operatorname{lcm}(D)$ then $a_m^{m/l}$ is uniquely determined by the $(a_d)_{d\in D}$.

Idea of proof. Let c be any generator of C_m and express each $a_d = (c^{m/d})^{r_d}$. With the ansatz $a_m = c^i$ translate the conditions on a_m to congruence equations for i modulo all $d \in D$ and $m/l/\gcd(l, m)$. The compatibility conditions of the a_d ensure that the Chinese remainder theorem yields a solution. A solution can be constructed using the extended Euclidean algorithm.

Compatible Generators of Cyclic Groups

$m \in \mathbb{N}$, C_m: cyclic group of order m

Definition. Let D be a set of divisors of m, closed under gcd. We call $(a_d)_{d\in D}$ a set of compatible generators for D, if each $a_d \in C_m$ has order d and

$$a_d^{d/d'} = a_{d'} \text{ for all } d, d' \in D \text{ with } d' \mid d.$$

Proposition. Assume $m \notin D$ and let $(a_d)_{d\in D}$ be a set of compatible generators for D. Then there exists $a_m \in C_m$ of order m with $a_m^{m/d} = a_d$ for all $d \in D$. If $l = \operatorname{lcm}(D)$ then $a_m^{m/l}$ is uniquely determined by the $(a_d)_{d\in D}$.

Idea of proof. Let c be any generator of C_m and express each $a_d = (c^{m/d})^{r_d}$. With the ansatz $a_m = c^i$ translate the conditions on a_m to congruence equations for i modulo all $d \in D$ and $m/l/\gcd(l, m)$. The compatibility conditions of the a_d ensure that the Chinese remainder theorem yields a solution. A solution can be constructed using the extended Euclidean algorithm.

Compatible Generators of Cyclic Groups

$m \in \mathbb{N}$, C_m: cyclic group of order m

Definition. Let D be a set of divisors of m, closed under gcd. We call $(a_d)_{d\in D}$ a set of compatible generators for D, if each $a_d \in C_m$ has order d and

$$a_d^{d/d'} = a_{d'} \text{ for all } d, d' \in D \text{ with } d' \mid d.$$

Proposition. Assume $m \notin D$ and let $(a_d)_{d\in D}$ be a set of compatible generators for D. Then there exists $a_m \in C_m$ of order m with $a_m^{m/d} = a_d$ for all $d \in D$. If $l = \operatorname{lcm}(D)$ then $a_m^{m/l}$ is uniquely determined by the $(a_d)_{d\in D}$.

Idea of proof. Let c be any generator of C_m and express each $a_d = (c^{m/d})^{r_d}$. With the ansatz $a_m = c^i$ translate the conditions on a_m to congruence equations for i modulo all $d \in D$ and $m/l/\gcd(l, m)$. The compatibility conditions of the a_d ensure that the Chinese remainder theorem yields a solution. A solution can be constructed using the extended Euclidean algorithm.

Compatible Generators of Cyclic Groups

$m \in \mathbb{N}$, C_m: cyclic group of order m

Definition. Let D be a set of divisors of m, closed under gcd. We call $(a_d)_{d\in D}$ a set of compatible generators for D, if each $a_d \in C_m$ has order d and

$$a_d^{d/d'} = a_{d'} \text{ for all } d, d' \in D \text{ with } d' \mid d.$$

Proposition. Assume $m \notin D$ and let $(a_d)_{d\in D}$ be a set of compatible generators for D. Then there exists $a_m \in C_m$ of order m with $a_m^{m/d} = a_d$ for all $d \in D$. If $l = \operatorname{lcm}(D)$ then $a_m^{m/l}$ is uniquely determined by the $(a_d)_{d\in D}$.

Idea of proof. Let c be any generator of C_m and express each $a_d = (c^{m/d})^{r_d}$. With the ansatz $a_m = c^i$ translate the conditions on a_m to congruence equations for i modulo all $d \in D$ and $m/l/\gcd(l, m)$. The compatibility conditions of the a_d ensure that the Chinese remainder theorem yields a solution. A solution can be constructed using the extended Euclidean algorithm.

Compatible Generators of Cyclic Groups

$m \in \mathbb{N}$, C_m: cyclic group of order m

Definition. Let D be a set of divisors of m, closed under gcd. We call $(a_d)_{d\in D}$ a set of compatible generators for D, if each $a_d \in C_m$ has order d and

$$a_d^{d/d'} = a_{d'} \text{ for all } d, d' \in D \text{ with } d' \mid d.$$

Proposition. Assume $m \notin D$ and let $(a_d)_{d\in D}$ be a set of compatible generators for D. Then there exists $a_m \in C_m$ of order m with $a_m^{m/d} = a_d$ for all $d \in D$. If $l = \operatorname{lcm}(D)$ then $a_m^{m/l}$ is uniquely determined by the $(a_d)_{d\in D}$.

Idea of proof. Let c be any generator of C_m and express each $a_d = (c^{m/d})^{r_d}$. With the ansatz $a_m = c^i$ translate the conditions on a_m to congruence equations for i modulo all $d \in D$ and $m/l/\gcd(l, m)$. The compatibility conditions of the a_d ensure that the Chinese remainder theorem yields a solution. A solution can be constructed using the extended Euclidean algorithm.

Finite Fields

p prime, $n \in \mathbb{N}$

- There exists finite field $\mathrm{GF}(p^n)$ of order p^n, unique up to isomorphism ($\mathrm{GF}(p) \cong \mathbb{Z}/p\mathbb{Z}$).
- $\mathrm{GF}(p^n)^\times$ is cyclic of order $p^n - 1$, generators are called primitive roots.
- $\mathrm{GF}(p^n) \cong \mathrm{GF}(p)[X]/(f(X))$ for any irreducible $f \in \mathrm{GF}(p)[X]$ of degree n.
- $\mathrm{GF}(p^d) \leq \mathrm{GF}(p^n)$ iff $d \mid n$, then $\mathrm{GF}(p^d)^\times = \{x \in \mathrm{GF}(p^n)^\times \mid x^{(p^d-1)} = 1\}$.
- For $d \mid n$ the extension $\mathrm{GF}(p^n)/\mathrm{GF}(p^d)$ is Galois with cyclic Galois group generated by $x \mapsto x^{(p^d)}$.

Finite Fields

p prime, $n \in \mathbb{N}$

- There exists finite field $\mathrm{GF}(p^n)$ of order p^n, unique up to isomorphism ($\mathrm{GF}(p) \cong \mathbb{Z}/p\mathbb{Z}$).
- $\mathrm{GF}(p^n)^\times$ is cyclic of order $p^n - 1$, generators are called primitive roots.
- $\mathrm{GF}(p^n) \cong \mathrm{GF}(p)[X]/(f(X))$ for any irreducible $f \in \mathrm{GF}(p)[X]$ of degree n.
- $\mathrm{GF}(p^d) \leq \mathrm{GF}(p^n)$ iff $d \mid n$, then $\mathrm{GF}(p^d)^\times = \{x \in \mathrm{GF}(p^n)^\times \mid x^{(p^d-1)} = 1\}$.
- For $d \mid n$ the extension $\mathrm{GF}(p^n)/\mathrm{GF}(p^d)$ is Galois with cyclic Galois group generated by $x \mapsto x^{(p^d)}$.

Finite Fields

p prime, $n \in \mathbb{N}$

- There exists finite field $\mathrm{GF}(p^n)$ of order p^n, unique up to isomorphism ($\mathrm{GF}(p) \cong \mathbb{Z}/p\mathbb{Z}$).
- $\mathrm{GF}(p^n)^\times$ is cyclic of order $p^n - 1$, generators are called primitive roots.
- $\mathrm{GF}(p^n) \cong \mathrm{GF}(p)[X]/(f(X))$ for any irreducible $f \in \mathrm{GF}(p)[X]$ of degree n.
- $\mathrm{GF}(p^d) \leq \mathrm{GF}(p^n)$ iff $d \mid n$, then $\mathrm{GF}(p^d)^\times = \{x \in \mathrm{GF}(p^n)^\times \mid x^{(p^d-1)} = 1\}$.
- For $d \mid n$ the extension $\mathrm{GF}(p^n)/\mathrm{GF}(p^d)$ is Galois with cyclic Galois group generated by $x \mapsto x^{(p^d)}$.

Finite Fields

p prime, $\quad n \in \mathbb{N}$

- There exists finite field $\mathrm{GF}(p^n)$ of order p^n, unique up to isomorphism ($\mathrm{GF}(p) \cong \mathbb{Z}/p\mathbb{Z}$).
- $\mathrm{GF}(p^n)^\times$ is cyclic of order $p^n - 1$, generators are called primitive roots.
- $\mathrm{GF}(p^n) \cong \mathrm{GF}(p)[X]/(f(X))$ for any irreducible $f \in \mathrm{GF}(p)[X]$ of degree n.
- $\mathrm{GF}(p^d) \leq \mathrm{GF}(p^n)$ iff $d \mid n$, then $\mathrm{GF}(p^d)^\times = \{x \in \mathrm{GF}(p^n)^\times \mid x^{(p^d-1)} = 1\}$.
- For $d \mid n$ the extension $\mathrm{GF}(p^n)/\mathrm{GF}(p^d)$ is Galois with cyclic Galois group generated by $x \mapsto x^{(p^d)}$.

Finite Fields

p prime, $\quad n \in \mathbb{N}$

- There exists finite field $\mathrm{GF}(p^n)$ of order p^n, unique up to isomorphism ($\mathrm{GF}(p) \cong \mathbb{Z}/p\mathbb{Z}$).
- $\mathrm{GF}(p^n)^\times$ is cyclic of order $p^n - 1$, generators are called primitive roots.
- $\mathrm{GF}(p^n) \cong \mathrm{GF}(p)[X]/(f(X))$ for any irreducible $f \in \mathrm{GF}(p)[X]$ of degree n.
- $\mathrm{GF}(p^d) \leq \mathrm{GF}(p^n)$ iff $d \mid n$, then $\mathrm{GF}(p^d)^\times = \{x \in \mathrm{GF}(p^n)^\times \mid x^{(p^d-1)} = 1\}$.
- For $d \mid n$ the extension $\mathrm{GF}(p^n)/\mathrm{GF}(p^d)$ is Galois with cyclic Galois group generated by $x \mapsto x^{(p^d)}$.

Finite Fields

p prime, $\quad n \in \mathbb{N}$

- There exists finite field $\mathrm{GF}(p^n)$ of order p^n, unique up to isomorphism ($\mathrm{GF}(p) \cong \mathbb{Z}/p\mathbb{Z}$).
- $\mathrm{GF}(p^n)^\times$ is cyclic of order $p^n - 1$, generators are called primitive roots.
- $\mathrm{GF}(p^n) \cong \mathrm{GF}(p)[X]/(f(X))$ for any irreducible $f \in \mathrm{GF}(p)[X]$ of degree n.
- $\mathrm{GF}(p^d) \leq \mathrm{GF}(p^n)$ iff $d \mid n$, then $\mathrm{GF}(p^d)^\times = \{x \in \mathrm{GF}(p^n)^\times \mid x^{(p^d-1)} = 1\}$.
- For $d \mid n$ the extension $\mathrm{GF}(p^n)/\mathrm{GF}(p^d)$ is Galois with cyclic Galois group generated by $x \mapsto x^{(p^d)}$.

Finite Fields

p prime, $\quad n \in \mathbb{N}$

- There exists finite field $\mathrm{GF}(p^n)$ of order p^n, unique up to isomorphism ($\mathrm{GF}(p) \cong \mathbb{Z}/p\mathbb{Z}$).
- $\mathrm{GF}(p^n)^\times$ is cyclic of order $p^n - 1$, generators are called primitive roots.
- $\mathrm{GF}(p^n) \cong \mathrm{GF}(p)[X]/(f(X))$ for any irreducible $f \in \mathrm{GF}(p)[X]$ of degree n.
- $\mathrm{GF}(p^d) \leq \mathrm{GF}(p^n)$ iff $d \mid n$, then $\mathrm{GF}(p^d)^\times = \{x \in \mathrm{GF}(p^n)^\times \mid x^{(p^d-1)} = 1\}$.
- For $d \mid n$ the extension $\mathrm{GF}(p^n)/\mathrm{GF}(p^d)$ is Galois with cyclic Galois group generated by $x \mapsto x^{(p^d)}$.

Conway polynomials

Definition. [R. Parker] A monic polynomial $C_{p,n}(X) \in \mathrm{GF}(p)[X]$ of degree n is called Conway polynomial iff

(1) $C_{p,n}(X)$ is irreducible and primitive (X has order $p^n - 1$ modulo $C_{p,n}(X)$).

(2) For $d \mid n$ we have $C_{p,d}(X^{(p^n-1)/(p^d-1)}) \equiv 0 \pmod{C_{p,n}(X)}$.

(3) $C_{p,n}(X)$ is the smallest polynomial with (1), (2) with respect to a certain ordering of $\mathrm{GF}(p)[X]$ ("signed lexicographic").

Remark. Conway polynomials exist: In algebraic closure K of $\mathrm{GF}(p)$ construct recursively for $n = 1, 2, \ldots$ compatible primitive roots x_n of $\mathrm{GF}(p^n)^\times$ with respect to the divisors $\{p^d - 1 \mid d \mid n, d < n\}$. In each step choose a compatible element with the smallest minimal polynomial over $\mathrm{GF}(p)$ (in ordering mentioned in (3)). The minimal polynomials of the x_n over $\mathrm{GF}(p)$ are the Conway polynomials.

Conway polynomials

Definition. [R. Parker] A monic polynomial $C_{p,n}(X) \in \mathrm{GF}(p)[X]$ of degree n is called Conway polynomial iff

(1) $C_{p,n}(X)$ is irreducible and primitive (X has order $p^n - 1$ modulo $C_{p,n}(X)$).

(2) For $d \mid n$ we have $C_{p,d}(X^{(p^n-1)/(p^d-1)}) \equiv 0 \pmod{C_{p,n}(X)}$.

(3) $C_{p,n}(X)$ is the smallest polynomial with (1), (2) with respect to a certain ordering of $\mathrm{GF}(p)[X]$ ("signed lexicographic").

Remark. Conway polynomials exist: In algebraic closure K of $\mathrm{GF}(p)$ construct recursively for $n = 1, 2, \ldots$ compatible primitive roots x_n of $\mathrm{GF}(p^n)^\times$ with respect to the divisors $\{p^d - 1 \mid d \mid n, d < n\}$. In each step choose a compatible element with the smallest minimal polynomial over $\mathrm{GF}(p)$ (in ordering mentioned in (3)). The minimal polynomials of the x_n over $\mathrm{GF}(p)$ are the Conway polynomials.

Conway polynomials

Definition. [R. Parker] A monic polynomial $C_{p,n}(X) \in \mathrm{GF}(p)[X]$ of degree n is called Conway polynomial iff

(1) $C_{p,n}(X)$ is irreducible and primitive (X has order $p^n - 1$ modulo $C_{p,n}(X)$).

(2) For $d \mid n$ we have $C_{p,d}(X^{(p^n-1)/(p^d-1)}) \equiv 0 \pmod{C_{p,n}(X)}$.

(3) $C_{p,n}(X)$ is the smallest polynomial with (1), (2) with respect to a certain ordering of $\mathrm{GF}(p)[X]$ ("signed lexicographic").

Remark. Conway polynomials exist: In algebraic closure K of $\mathrm{GF}(p)$ construct recursively for $n = 1, 2, \ldots$ compatible primitive roots x_n of $\mathrm{GF}(p^n)^\times$ with respect to the divisors $\{p^d - 1 \mid d \mid n, d < n\}$. In each step choose a compatible element with the smallest minimal polynomial over $\mathrm{GF}(p)$ (in ordering mentioned in (3)). The minimal polynomials of the x_n over $\mathrm{GF}(p)$ are the Conway polynomials.

Conway polynomials

Definition. [R. Parker] A monic polynomial $C_{p,n}(X) \in \mathrm{GF}(p)[X]$ of degree n is called Conway polynomial iff

(1) $C_{p,n}(X)$ is irreducible and primitive (X has order $p^n - 1$ modulo $C_{p,n}(X)$).

(2) For $d \mid n$ we have $C_{p,d}(X^{(p^n-1)/(p^d-1)}) \equiv 0 \pmod{C_{p,n}(X)}$.

(3) $C_{p,n}(X)$ is the smallest polynomial with (1), (2) with respect to a certain ordering of $\mathrm{GF}(p)[X]$ ("signed lexicographic").

Remark. Conway polynomials exist: In algebraic closure K of $\mathrm{GF}(p)$ construct recursively for $n = 1, 2, \ldots$ compatible primitive roots x_n of $\mathrm{GF}(p^n)^\times$ with respect to the divisors $\{p^d - 1 \mid d \mid n, d < n\}$. In each step choose a compatible element with the smallest minimal polynomial over $\mathrm{GF}(p)$ (in ordering mentioned in (3)). The minimal polynomials of the x_n over $\mathrm{GF}(p)$ are the Conway polynomials.

Conway polynomials

Definition. [R. Parker] A monic polynomial $C_{p,n}(X) \in \mathrm{GF}(p)[X]$ of degree n is called Conway polynomial iff

(1) $C_{p,n}(X)$ is irreducible and primitive (X has order $p^n - 1$ modulo $C_{p,n}(X)$).

(2) For $d \mid n$ we have $C_{p,d}(X^{(p^n-1)/(p^d-1)}) \equiv 0 \pmod{C_{p,n}(X)}$.

(3) $C_{p,n}(X)$ is the smallest polynomial with (1), (2) with respect to a certain ordering of $\mathrm{GF}(p)[X]$ ("signed lexicographic").

Remark. Conway polynomials exist: In algebraic closure K of $\mathrm{GF}(p)$ construct recursively for $n = 1, 2, \ldots$ compatible primitive roots x_n of $\mathrm{GF}(p^n)^\times$ with respect to the divisors $\{p^d - 1 \mid d \mid n, d < n\}$. In each step choose a compatible element with the smallest minimal polynomial over $\mathrm{GF}(p)$ (in ordering mentioned in (3)). The minimal polynomials of the x_n over $\mathrm{GF}(p)$ are the Conway polynomials.

Conway polynomials

Definition. [R. Parker] A monic polynomial $C_{p,n}(X) \in \mathrm{GF}(p)[X]$ of degree n is called Conway polynomial iff

(1) $C_{p,n}(X)$ is irreducible and primitive (X has order $p^n - 1$ modulo $C_{p,n}(X)$).

(2) For $d \mid n$ we have $C_{p,d}(X^{(p^n-1)/(p^d-1)}) \equiv 0 \pmod{C_{p,n}(X)}$.

(3) $C_{p,n}(X)$ is the smallest polynomial with (1), (2) with respect to a certain ordering of $\mathrm{GF}(p)[X]$ ("signed lexicographic").

Remark. Conway polynomials exist: In algebraic closure K of $\mathrm{GF}(p)$ construct recursively for $n = 1, 2, \ldots$ compatible primitive roots x_n of $\mathrm{GF}(p^n)^\times$ with respect to the divisors $\{p^d - 1 \mid d \mid n, d < n\}$. In each step choose a compatible element with the smallest minimal polynomial over $\mathrm{GF}(p)$ (in ordering mentioned in (3)). The minimal polynomials of the x_n over $\mathrm{GF}(p)$ are the Conway polynomials.

Motivation

(a) Conway polynomials define an embedding $\overline{\mathrm{GF}(p)}^{\times} \to \mathbb{C}^{\times}$, with $x_n \mapsto \exp(2\pi i/(p^n-1))$ for each $n \in \mathbb{N}$.
- Defines lifting of eigenvalues for Brauer characters.
- Inverse map defines reduction of ordinary characters mod p (i.e., a choice of a p-modular system).
- Useful to fix this embedding once and for all, for example for data concerning representations of finite groups, like the Atlas of Brauer characters, collections of representations, ...

(b) One can compute in some $\mathrm{GF}(p^{n_i})$ and later embed easily all elements into a larger $\mathrm{GF}(p^n)$ with $n_i \mid n$ for all i.

(c) Makes exchange of data containing finite field elements easier.

Remarks.
- The primitivity condition in the definition is needed for (a), while (b), (c) could be achieved easier.
- A list of (all) known Conway polynomials in on my Webpage.
- They are used in Sage, GAP, Magma, MeatAxe, Atlas, ...

Motivation

(a) Conway polynomials define an embedding $\overline{\mathrm{GF}(p)}^{\times} \to \mathbb{C}^{\times}$, with $x_n \mapsto \exp(2\pi i/(p^n-1))$ for each $n \in \mathbb{N}$.

- Defines lifting of eigenvalues for Brauer characters.
- Inverse map defines reduction of ordinary characters mod p (i.e., a choice of a p-modular system).
- Useful to fix this embedding once and for all, for example for data concerning representations of finite groups, like the Atlas of Brauer characters, collections of representations, ...

(b) One can compute in some $\mathrm{GF}(p^{n_i})$ and later embed easily all elements into a larger $\mathrm{GF}(p^n)$ with $n_i \mid n$ for all i.

(c) Makes exchange of data containing finite field elements easier.

Remarks.

- The primitivity condition in the definition is needed for (a), while (b), (c) could be achieved easier.
- A list of (all) known Conway polynomials in on my Webpage.
- They are used in Sage, GAP, Magma, MeatAxe, Atlas, ...

Motivation

(a) Conway polynomials define an embedding $\overline{\mathrm{GF}(p)}^{\times} \to \mathbb{C}^{\times}$, with $x_n \mapsto \exp(2\pi i/(p^n-1))$ for each $n \in \mathbb{N}$.
- Defines lifting of eigenvalues for Brauer characters.
- Inverse map defines reduction of ordinary characters mod p (i.e., a choice of a p-modular system).
- Useful to fix this embedding once and for all, for example for data concerning representations of finite groups, like the Atlas of Brauer characters, collections of representations, ...

(b) One can compute in some $\mathrm{GF}(p^{n_i})$ and later embed easily all elements into a larger $\mathrm{GF}(p^n)$ with $n_i \mid n$ for all i.

(c) Makes exchange of data containing finite field elements easier.

Remarks.
- The primitivity condition in the definition is needed for (a), while (b), (c) could be achieved easier.
- A list of (all) known Conway polynomials in on my Webpage.
- They are used in Sage, GAP, Magma, MeatAxe, Atlas, ...

Motivation

(a) Conway polynomials define an embedding $\overline{\mathrm{GF}(p)}^{\times} \to \mathbb{C}^{\times}$, with $x_n \mapsto \exp(2\pi i/(p^n-1))$ for each $n \in \mathbb{N}$.
- Defines lifting of eigenvalues for Brauer characters.
- Inverse map defines reduction of ordinary characters mod p (i.e., a choice of a p-modular system).
- Useful to fix this embedding once and for all, for example for data concerning representations of finite groups, like the Atlas of Brauer characters, collections of representations, ...

(b) One can compute in some $\mathrm{GF}(p^{n_i})$ and later embed easily all elements into a larger $\mathrm{GF}(p^n)$ with $n_i \mid n$ for all i.

(c) Makes exchange of data containing finite field elements easier.

Remarks.
- The primitivity condition in the definition is needed for (a), while (b), (c) could be achieved easier.
- A list of (all) known Conway polynomials in on my Webpage.
- They are used in Sage, GAP, Magma, MeatAxe, Atlas, ...

Motivation

(a) Conway polynomials define an embedding $\overline{\mathrm{GF}(p)}^{\times} \to \mathbb{C}^{\times}$, with $x_n \mapsto \exp(2\pi i/(p^n-1))$ for each $n \in \mathbb{N}$.
- Defines lifting of eigenvalues for Brauer characters.
- Inverse map defines reduction of ordinary characters mod p (i.e., a choice of a p-modular system).
- Useful to fix this embedding once and for all, for example for data concerning representations of finite groups, like the Atlas of Brauer characters, collections of representations, ...

(b) One can compute in some $\mathrm{GF}(p^{n_i})$ and later embed easily all elements into a larger $\mathrm{GF}(p^n)$ with $n_i \mid n$ for all i.

(c) Makes exchange of data containing finite field elements easier.

Remarks.
- The primitivity condition in the definition is needed for (a), while (b), (c) could be achieved easier.
- A list of (all) known Conway polynomials in on my Webpage.
- They are used in Sage, GAP, Magma, MeatAxe, Atlas, ...

Motivation

(a) Conway polynomials define an embedding $\overline{\mathrm{GF}(p)}^{\times} \to \mathbb{C}^{\times}$, with $x_n \mapsto \exp(2\pi i/(p^n-1))$ for each $n \in \mathbb{N}$.
- Defines lifting of eigenvalues for Brauer characters.
- Inverse map defines reduction of ordinary characters mod p (i.e., a choice of a p-modular system).
- Useful to fix this embedding once and for all, for example for data concerning representations of finite groups, like the Atlas of Brauer characters, collections of representations, ...

(b) One can compute in some $\mathrm{GF}(p^{n_i})$ and later embed easily all elements into a larger $\mathrm{GF}(p^n)$ with $n_i \mid n$ for all i.

(c) Makes exchange of data containing finite field elements easier.

Remarks.
- The primitivity condition in the definition is needed for (a), while (b), (c) could be achieved easier.
- A list of (all) known Conway polynomials in on my Webpage.
- They are used in Sage, GAP, Magma, MeatAxe, Atlas, ...

Motivation

(a) Conway polynomials define an embedding $\overline{\mathrm{GF}(p)}^{\times} \to \mathbb{C}^{\times}$, with $x_n \mapsto \exp(2\pi i/(p^n-1))$ for each $n \in \mathbb{N}$.
- Defines lifting of eigenvalues for Brauer characters.
- Inverse map defines reduction of ordinary characters mod p (i.e., a choice of a p-modular system).
- Useful to fix this embedding once and for all, for example for data concerning representations of finite groups, like the Atlas of Brauer characters, collections of representations, ...

(b) One can compute in some $\mathrm{GF}(p^{n_i})$ and later embed easily all elements into a larger $\mathrm{GF}(p^n)$ with $n_i \mid n$ for all i.

(c) Makes exchange of data containing finite field elements easier.

Remarks.
- The primitivity condition in the definition is needed for (a), while (b), (c) could be achieved easier.
- A list of (all) known Conway polynomials in on my Webpage.
- They are used in Sage, GAP, Magma, MeatAxe, Atlas, ...

Motivation

(a) Conway polynomials define an embedding $\overline{\mathrm{GF}(p)}^{\times} \to \mathbb{C}^{\times}$, with $x_n \mapsto \exp(2\pi i/(p^n-1))$ for each $n \in \mathbb{N}$.
- Defines lifting of eigenvalues for Brauer characters.
- Inverse map defines reduction of ordinary characters mod p (i.e., a choice of a p-modular system).
- Useful to fix this embedding once and for all, for example for data concerning representations of finite groups, like the Atlas of Brauer characters, collections of representations, ...

(b) One can compute in some $\mathrm{GF}(p^{n_i})$ and later embed easily all elements into a larger $\mathrm{GF}(p^n)$ with $n_i \mid n$ for all i.

(c) Makes exchange of data containing finite field elements easier.

Remarks.
- The primitivity condition in the definition is needed for (a), while (b), (c) could be achieved easier.
- A list of (all) known Conway polynomials in on my Webpage.
- They are used in Sage, GAP, Magma, MeatAxe, Atlas, ...

Motivation

(a) Conway polynomials define an embedding $\overline{\mathrm{GF}(p)}^{\times} \to \mathbb{C}^{\times}$, with $x_n \mapsto \exp(2\pi i/(p^n-1))$ for each $n \in \mathbb{N}$.
- Defines lifting of eigenvalues for Brauer characters.
- Inverse map defines reduction of ordinary characters mod p (i.e., a choice of a p-modular system).
- Useful to fix this embedding once and for all, for example for data concerning representations of finite groups, like the Atlas of Brauer characters, collections of representations, ...

(b) One can compute in some $\mathrm{GF}(p^{n_i})$ and later embed easily all elements into a larger $\mathrm{GF}(p^n)$ with $n_i \mid n$ for all i.

(c) Makes exchange of data containing finite field elements easier.

Remarks.
- The primitivity condition in the definition is needed for (a), while (b), (c) could be achieved easier.
- A list of (all) known Conway polynomials in on my Webpage.
- They are used in Sage, GAP, Magma, MeatAxe, Atlas, ...

Motivation

(a) Conway polynomials define an embedding $\overline{\mathrm{GF}(p)}^{\times} \to \mathbb{C}^{\times}$, with $x_n \mapsto \exp(2\pi i/(p^n-1))$ for each $n \in \mathbb{N}$.
- Defines lifting of eigenvalues for Brauer characters.
- Inverse map defines reduction of ordinary characters mod p (i.e., a choice of a p-modular system).
- Useful to fix this embedding once and for all, for example for data concerning representations of finite groups, like the Atlas of Brauer characters, collections of representations, ...

(b) One can compute in some $\mathrm{GF}(p^{n_i})$ and later embed easily all elements into a larger $\mathrm{GF}(p^n)$ with $n_i \mid n$ for all i.

(c) Makes exchange of data containing finite field elements easier.

Remarks.
- The primitivity condition in the definition is needed for (a), while (b), (c) could be achieved easier.
- A list of (all) known Conway polynomials in on my Webpage.
- They are used in Sage, GAP, Magma, MeatAxe, Atlas, ...

Motivation

(a) Conway polynomials define an embedding $\overline{\mathrm{GF}(p)}^{\times} \to \mathbb{C}^{\times}$, with $x_n \mapsto \exp(2\pi i/(p^n-1))$ for each $n \in \mathbb{N}$.
- Defines lifting of eigenvalues for Brauer characters.
- Inverse map defines reduction of ordinary characters mod p (i.e., a choice of a p-modular system).
- Useful to fix this embedding once and for all, for example for data concerning representations of finite groups, like the Atlas of Brauer characters, collections of representations, ...

(b) One can compute in some $\mathrm{GF}(p^{n_i})$ and later embed easily all elements into a larger $\mathrm{GF}(p^n)$ with $n_i \mid n$ for all i.

(c) Makes exchange of data containing finite field elements easier.

Remarks.
- The primitivity condition in the definition is needed for (a), while (b), (c) could be achieved easier.
- A list of (all) known Conway polynomials in on my Webpage.
- They are used in Sage, GAP, Magma, MeatAxe, Atlas, ...

Primitivity

Primitivity of a monic polynomial $f(X) \in \mathrm{GF}(p)[X]$ of degree n can be checked using the following Lemma.

Lemma. $f(X)$ is irreducible and primitive iff $X^{(p^n-1)/r} \neq 1 \pmod{f(X)}$ for all prime divisors r of $p^n - 1$.

(High powers are computed by repeated squaring method.)

Primitivity can only be checked if the prime factorization of $p^n - 1$ is known.

For $p < 10000$ there are about 24200 pairs (p, n) such that the factorization of $p^n - 1$ is known (using collections of factors of numbers of form $a^k \pm 1$ by Cunningham, Brent, Montgomery, te Riele, and others—these are available in GAP and Magma).

We would like to know the Conway polynomials in all these 24200 cases.

Primitivity

Primitivity of a monic polynomial $f(X) \in \mathrm{GF}(p)[X]$ of degree n can be checked using the following Lemma.

Lemma. $f(X)$ is irreducible and primitive iff $X^{(p^n-1)/r} \neq 1 \pmod{f(X)}$ for all prime divisors r of $p^n - 1$.

(High powers are computed by repeated squaring method.)

Primitivity can only be checked if the prime factorization of $p^n - 1$ is known.

For $p < 10000$ there are about 24200 pairs (p, n) such that the factorization of $p^n - 1$ is known (using collections of factors of numbers of form $a^k \pm 1$ by Cunningham, Brent, Montgomery, te Riele, and others—these are available in GAP and Magma).

We would like to know the Conway polynomials in all these 24200 cases.

Primitivity

Primitivity of a monic polynomial $f(X) \in \mathrm{GF}(p)[X]$ of degree n can be checked using the following Lemma.

Lemma. $f(X)$ is irreducible and primitive iff $X^{(p^n-1)/r} \neq 1 \pmod{f(X)}$ for all prime divisors r of $p^n - 1$.

(High powers are computed by repeated squaring method.)

Primitivity can only be checked if the prime factorization of $p^n - 1$ is known.

For $p < 10000$ there are about 24200 pairs (p, n) such that the factorization of $p^n - 1$ is known (using collections of factors of numbers of form $a^k \pm 1$ by Cunningham, Brent, Montgomery, te Riele, and others—these are available in GAP and Magma).

We would like to know the Conway polynomials in all these 24200 cases.

Primitivity

Primitivity of a monic polynomial $f(X) \in \mathrm{GF}(p)[X]$ of degree n can be checked using the following Lemma.

Lemma. $f(X)$ is irreducible and primitive iff $X^{(p^n-1)/r} \neq 1 \pmod{f(X)}$ for all prime divisors r of $p^n - 1$.

(High powers are computed by repeated squaring method.)

Primitivity can only be checked if the prime factorization of $p^n - 1$ is known.

For $p < 10000$ there are about 24200 pairs (p, n) such that the factorization of $p^n - 1$ is known (using collections of factors of numbers of form $a^k \pm 1$ by Cunningham, Brent, Montgomery, te Riele, and others—these are available in GAP and Magma).

We would like to know the Conway polynomials in all these 24200 cases.

Primitivity

Primitivity of a monic polynomial $f(X) \in \mathrm{GF}(p)[X]$ of degree n can be checked using the following Lemma.

Lemma. $f(X)$ is irreducible and primitive iff $X^{(p^n-1)/r} \neq 1 \pmod{f(X)}$ for all prime divisors r of $p^n - 1$.

(High powers are computed by repeated squaring method.)

Primitivity can only be checked if the prime factorization of $p^n - 1$ is known.

For $p < 10000$ there are about 24200 pairs (p, n) such that the factorization of $p^n - 1$ is known (using collections of factors of numbers of form $a^k \pm 1$ by Cunningham, Brent, Montgomery, te Riele, and others—these are available in GAP and Magma).

We would like to know the Conway polynomials in all these 24200 cases.

Primitivity

Primitivity of a monic polynomial $f(X) \in \mathrm{GF}(p)[X]$ of degree n can be checked using the following Lemma.

Lemma. $f(X)$ is irreducible and primitive iff $X^{(p^n-1)/r} \neq 1 \pmod{f(X)}$ for all prime divisors r of $p^n - 1$.

(High powers are computed by repeated squaring method.)

Primitivity can only be checked if the prime factorization of $p^n - 1$ is known.

For $p < 10000$ there are about 24200 pairs (p, n) such that the factorization of $p^n - 1$ is known (using collections of factors of numbers of form $a^k \pm 1$ by Cunningham, Brent, Montgomery, te Riele, and others—these are available in GAP and Magma).

We would like to know the Conway polynomials in all these 24200 cases.

Primitivity

Primitivity of a monic polynomial $f(X) \in \mathrm{GF}(p)[X]$ of degree n can be checked using the following Lemma.

Lemma. $f(X)$ is irreducible and primitive iff $X^{(p^n-1)/r} \neq 1 \pmod{f(X)}$ for all prime divisors r of $p^n - 1$.

(High powers are computed by repeated squaring method.)

Primitivity can only be checked if the prime factorization of $p^n - 1$ is known.

For $p < 10000$ there are about 24200 pairs (p, n) such that the factorization of $p^n - 1$ is known (using collections of factors of numbers of form $a^k \pm 1$ by Cunningham, Brent, Montgomery, te Riele, and others—these are available in GAP and Magma).

We would like to know the Conway polynomials in all these 24200 cases.

Computation of Conway polynomials

Two main methods:

(a) Enumerate polynomials and check primitivity and compatibility.

(b) Enumerate all compatible primitive roots, compute their minimal polynomial to find smallest.

Remarks.

- There are $(p^n - 1)/\mathrm{lcm}(p^d - 1 \mid d \mid n, d < n)$ compatible elements.
- Compatibility for $d = 1$ determines the constant term of $C_{p,n}(X)$.
- Method (a) is good if n is a prime (about n polynomials to check). But:
- Only about 3800 Conway polynomials are known, they were computed in decades of CPU-time (R.Parker, T.Breuer, F.L., J.Bray, K.Minola).
- Further ones of non-prime degree are almost impossible to find.

Computation of Conway polynomials

Two main methods:

(a) Enumerate polynomials and check primitivity and compatibility.

(b) Enumerate all compatible primitive roots, compute their minimal polynomial to find smallest.

Remarks.

- There are $(p^n - 1)/\mathrm{lcm}(p^d - 1 \mid d \mid n, d < n)$ compatible elements.
- Compatibility for $d = 1$ determines the constant term of $C_{p,n}(X)$.
- Method (a) is good if n is a prime (about n polynomials to check). But:
- Only about 3800 Conway polynomials are known, they were computed in decades of CPU-time (R.Parker, T.Breuer, F.L., J.Bray, K.Minola).
- Further ones of non-prime degree are almost impossible to find.

Computation of Conway polynomials

Two main methods:

(a) Enumerate polynomials and check primitivity and compatibility.

(b) Enumerate all compatible primitive roots, compute their minimal polynomial to find smallest.

Remarks.

- There are $(p^n - 1)/\mathrm{lcm}(p^d - 1 \mid d \mid n, d < n)$ compatible elements.
- Compatibility for $d = 1$ determines the constant term of $C_{p,n}(X)$.
- Method (a) is good if n is a prime (about n polynomials to check). But:
- Only about 3800 Conway polynomials are known, they were computed in decades of CPU-time (R.Parker, T.Breuer, F.L., J.Bray, K.Minola).
- Further ones of non-prime degree are almost impossible to find.

Computation of Conway polynomials

Two main methods:

(a) Enumerate polynomials and check primitivity and compatibility.

(b) Enumerate all compatible primitive roots, compute their minimal polynomial to find smallest.

Remarks.

- There are $(p^n - 1)/\mathrm{lcm}(p^d - 1 \mid d \mid n, d < n)$ compatible elements.
- Compatibility for $d = 1$ determines the constant term of $C_{p,n}(X)$.
- Method (a) is good if n is a prime (about n polynomials to check). But:
- Only about 3800 Conway polynomials are known, they were computed in decades of CPU-time (R.Parker, T.Breuer, F.L., J.Bray, K.Minola).
- Further ones of non-prime degree are almost impossible to find.

Computation of Conway polynomials

Two main methods:

(a) Enumerate polynomials and check primitivity and compatibility.

(b) Enumerate all compatible primitive roots, compute their minimal polynomial to find smallest.

Remarks.

- There are $(p^n - 1)/\mathrm{lcm}(p^d - 1 \mid d \mid n, d < n)$ compatible elements.
- Compatibility for $d = 1$ determines the constant term of $C_{p,n}(X)$.
- Method (a) is good if n is a prime (about n polynomials to check). But:
- Only about 3800 Conway polynomials are known, they were computed in decades of CPU-time (R.Parker, T.Breuer, F.L., J.Bray, K.Minola).
- Further ones of non-prime degree are almost impossible to find.

Computation of Conway polynomials

Two main methods:

(a) Enumerate polynomials and check primitivity and compatibility.

(b) Enumerate all compatible primitive roots, compute their minimal polynomial to find smallest.

Remarks.

- There are $(p^n - 1)/\mathrm{lcm}(p^d - 1 \mid d \mid n, d < n)$ compatible elements.
- Compatibility for $d = 1$ determines the constant term of $C_{p,n}(X)$.
- Method (a) is good if n is a prime (about n polynomials to check). But:
- Only about 3800 Conway polynomials are known, they were computed in decades of CPU-time (R.Parker, T.Breuer, F.L., J.Bray, K.Minola).
- Further ones of non-prime degree are almost impossible to find.

Computation of Conway polynomials

Two main methods:

(a) Enumerate polynomials and check primitivity and compatibility.

(b) Enumerate all compatible primitive roots, compute their minimal polynomial to find smallest.

Remarks.

- There are $(p^n - 1)/\mathrm{lcm}(p^d - 1 \mid d \mid n, d < n)$ compatible elements.
- Compatibility for $d = 1$ determines the constant term of $C_{p,n}(X)$.
- Method (a) is good if n is a prime (about n polynomials to check). But:
- Only about 3800 Conway polynomials are known, they were computed in decades of CPU-time (R.Parker, T.Breuer, F.L., J.Bray, K.Minola).
- Further ones of non-prime degree are almost impossible to find.

Computation of Conway polynomials

Two main methods:

(a) Enumerate polynomials and check primitivity and compatibility.

(b) Enumerate all compatible primitive roots, compute their minimal polynomial to find smallest.

Remarks.

- There are $(p^n - 1)/\mathrm{lcm}(p^d - 1 \mid d \mid n, d < n)$ compatible elements.
- Compatibility for $d = 1$ determines the constant term of $C_{p,n}(X)$.
- Method (a) is good if n is a prime (about n polynomials to check). But:
- Only about 3800 Conway polynomials are known, they were computed in decades of CPU-time (R.Parker, T.Breuer, F.L., J.Bray, K.Minola).
- Further ones of non-prime degree are almost impossible to find.

Modified Conway polynomials

Idea. Modify the definition of Conway polynomials such that they can be computed in practive whenever the factorization of $p^n - 1$ is known.

Substitute the minimality condition for Conway polynomials by a description of how to compute one compatible polynomial.

We compute for each fixed prime p recursively modified polynomials $C'_{p,n}(X) \in \mathrm{GF}(p)[X]$ and a set of compatible primitive roots of the $\mathrm{GF}(p^n)$.

Modified Conway polynomials

Idea. Modify the definition of Conway polynomials such that they can be computed in practive whenever the factorization of $p^n - 1$ is known.

Substitute the minimality condition for Conway polynomials by a description of how to compute one compatible polynomial.

We compute for each fixed prime p recursively modified polynomials $C'_{p,n}(X) \in \mathrm{GF}(p)[X]$ and a set of compatible primitive roots of the $\mathrm{GF}(p^n)$.

Modified Conway polynomials

Idea. Modify the definition of Conway polynomials such that they can be computed in practive whenever the factorization of $p^n - 1$ is known.

Substitute the minimality condition for Conway polynomials by a description of how to compute one compatible polynomial.

We compute for each fixed prime p recursively modified polynomials $C'_{p,n}(X) \in \mathrm{GF}(p)[X]$ and a set of compatible primitive roots of the $\mathrm{GF}(p^n)$.

Modified Conway polynomials

Idea. Modify the definition of Conway polynomials such that they can be computed in practive whenever the factorization of $p^n - 1$ is known.

Substitute the minimality condition for Conway polynomials by a description of how to compute one compatible polynomial.

We compute for each fixed prime p recursively modified polynomials $C'_{p,n}(X) \in \mathrm{GF}(p)[X]$ and a set of compatible primitive roots of the $\mathrm{GF}(p^n)$.

- If $C_{p,n}(X)$ is known, or $n = 4$ or n is a prime: use old definition, $C'_{p,n}(X) = C_{p,n}(X)$.
- If $n = l^a$ is a prime power (only one compatibility condition): Enumerate polynomials of degree l over $\mathrm{GF}(p^{(l^{a-1})})$ with correct constant term and check primitivity. If found compute minimal polynomial $C'_{p,n}(X)$ of its zero over $\mathrm{GF}(p)$. Choose $X + C'_{p,n}(X)$ as primitive root.
- Else $n = l_1^{a_1} \cdots l_k^{a_k}$ prime factorization of n with $k > 1$: Compute in

$$F = (\mathrm{GF}(p)[X_1]/(C'_{p,l_1^{a_1}}(X_1)))[X_2]/(C'_{p,l_2^{a_2}}(X_2)) \ldots$$

(k independent extensions of $\mathrm{GF}(p)$), find primitive root in basis of $\{X_1^{i_1} \cdots X_k^{i^k}\}$.

- If $C_{p,n}(X)$ is known, or $n = 4$ or n is a prime: use old definition, $C'_{p,n}(X) = C_{p,n}(X)$.
- If $n = l^a$ is a prime power (only one compatibility condition): Enumerate polynomials of degree l over $\mathrm{GF}(p^{(l^{a-1})})$ with correct constant term and check primitivity. If found compute minimal polynomial $C'_{p,n}(X)$ of its zero over $\mathrm{GF}(p)$. Choose $X + C'_{p,n}(X)$ as primitive root.
- Else $n = l_1^{a_1} \cdots l_k^{a_k}$ prime factorization of n with $k > 1$: Compute in

$$F = (\mathrm{GF}(p)[X_1]/(C'_{p,l_1^{a_1}}(X_1)))[X_2]/(C'_{p,l_2^{a_2}}(X_2)) \ldots$$

(k independent extensions of $\mathrm{GF}(p)$), find primitive root in basis of $\{X_1^{i_1} \cdots X_k^{i^k}\}$.

- If $C_{p,n}(X)$ is known, or $n = 4$ or n is a prime: use old definition, $C'_{p,n}(X) = C_{p,n}(X)$.
- If $n = l^a$ is a prime power (only one compatibility condition): Enumerate polynomials of degree l over $\mathrm{GF}(p^{(l^{a-1})})$ with correct constant term and check primitivity. If found compute minimal polynomial $C'_{p,n}(X)$ of its zero over $\mathrm{GF}(p)$. Choose $X + C'_{p,n}(X)$ as primitive root.
- Else $n = l_1^{a_1} \cdots l_k^{a_k}$ prime factorization of n with $k > 1$: Compute in

$$F = (\mathrm{GF}(p)[X_1]/(C'_{p,l_1^{a_1}}(X_1)))[X_2]/(C'_{p,l_2^{a_2}}(X_2)) \ldots$$

(k independent extensions of $\mathrm{GF}(p)$), find primitive root in basis of $\{X_1^{i_1} \cdots X_k^{i^k}\}$.

Details for case $n = l_1^{a_1} \cdots l_k^{a_k}, k > 1$:

- By recursion write down in F primitive roots of maximal subfields of order $p^{n_i}, n_i = n/l_i, 1 \le i \le k$.
- Compute the unique compatible element t of order $l = \mathrm{lcm}(p^{n_i} - 1, 1 \le i \le k)$.
- Using t search a primitive root z of F by a fixed algorithm.
- Compute a $(p^n - 1)/l$-th root x_n' of t by a fixed algorithm (always easy, because $\gcd(l, (p^n - 1)/l)$ is very small).
- Set $x_n = x_n' z^{lj}$ with minimal j such that x_n is primitive root. Then $C'_{p,n}(X)$ is the minimal polynomial of x_n over $\mathrm{GF}(p)$.

Details for case $n = l_1^{a_1} \cdots l_k^{a_k}, k > 1$:

- By recursion write down in F primitive roots of maximal subfields of order $p^{n_i}, n_i = n/l_i, 1 \le i \le k$.
- Compute the unique compatible element t of order $l = \mathrm{lcm}(p^{n_i} - 1, 1 \le i \le k)$.
- Using t search a primitive root z of F by a fixed algorithm.
- Compute a $(p^n - 1)/l$-th root x_n' of t by a fixed algorithm (always easy, because $\gcd(l, (p^n - 1)/l)$ is very small).
- Set $x_n = x_n' z^{lj}$ with minimal j such that x_n is primitive root. Then $C_{p,n}'(X)$ is the minimal polynomial of x_n over $\mathrm{GF}(p)$.

Details for case $n = l_1^{a_1} \cdots l_k^{a_k}, k > 1$:

- By recursion write down in F primitive roots of maximal subfields of order $p^{n_i}, n_i = n/l_i, 1 \le i \le k$.
- Compute the unique compatible element t of order $l = \mathrm{lcm}(p^{n_i} - 1, 1 \le i \le k)$.
- Using t search a primitive root z of F by a fixed algorithm.
- Compute a $(p^n - 1)/l$-th root x'_n of t by a fixed algorithm (always easy, because $\gcd(l, (p^n - 1)/l)$ is very small).
- Set $x_n = x'_n z^{lj}$ with minimal j such that x_n is primitive root. Then $C'_{p,n}(X)$ is the minimal polynomial of x_n over $\mathrm{GF}(p)$.

Details for case $n = l_1^{a_1} \cdots l_k^{a_k}, k > 1$:

- By recursion write down in F primitive roots of maximal subfields of order $p^{n_i}, n_i = n/l_i, 1 \le i \le k$.
- Compute the unique compatible element t of order $l = \mathrm{lcm}(p^{n_i} - 1, 1 \le i \le k)$.
- Using t search a primitive root z of F by a fixed algorithm.
- Compute a $(p^n - 1)/l$-th root x'_n of t by a fixed algorithm (always easy, because $\gcd(l, (p^n - 1)/l)$ is very small).
- Set $x_n = x'_n z^{lj}$ with minimal j such that x_n is primitive root. Then $C'_{p,n}(X)$ is the minimal polynomial of x_n over $\mathrm{GF}(p)$.

Details for case $n = l_1^{a_1} \cdots l_k^{a_k}, k > 1$:

- By recursion write down in F primitive roots of maximal subfields of order $p^{n_i}, n_i = n/l_i, 1 \le i \le k$.
- Compute the unique compatible element t of order $l = \mathrm{lcm}(p^{n_i} - 1, 1 \le i \le k)$.
- Using t search a primitive root z of F by a fixed algorithm.
- Compute a $(p^n - 1)/l$-th root x'_n of t by a fixed algorithm (always easy, because $\gcd(l, (p^n - 1)/l)$ is very small).
- Set $x_n = x'_n z^{lj}$ with minimal j such that x_n is primitive root. Then $C'_{p,n}(X)$ is the minimal polynomial of x_n over $\mathrm{GF}(p)$.

Details for case $n = l_1^{a_1} \cdots l_k^{a_k}$, $k > 1$:

- By recursion write down in F primitive roots of maximal subfields of order p^{n_i}, $n_i = n/l_i$, $1 \le i \le k$.
- Compute the unique compatible element t of order $l = \mathrm{lcm}(p^{n_i} - 1, 1 \le i \le k)$.
- Using t search a primitive root z of F by a fixed algorithm.
- Compute a $(p^n - 1)/l$-th root x'_n of t by a fixed algorithm (always easy, because $\gcd(l, (p^n - 1)/l)$ is very small).
- Set $x_n = x'_n z^{lj}$ with minimal j such that x_n is primitive root. Then $C'_{p,n}(X)$ is the minimal polynomial of x_n over $\mathrm{GF}(p)$.

Implementation

With an implementation in Magma all 24200 cases of $C'_{p,n}(X)$ with $p < 10000$ and known factorization of $p^n - 1$ could be computed over night.

Since the known $C_{p,n}(X)$ are still needed as explicit list it seems sensible to precompute and distribute all known $C'_{p,n}(X)$ in a similar way.

Keeping the known $C_{p,n}(X)$ as $C'_{p,n}(X)$ is necessary for backward compatibility: For example, it would be practically impossible to rewrite the character tables from the Modular Atlas in terms of another set of standard polynomials for finite fields.

We keep $C'_{p,4}(X) = C_{p,4}(X)$ because there is a quick algorithm to find these Conway polynomials (Bray).

Implementation

With an implementation in Magma all 24200 cases of $C'_{p,n}(X)$ with $p < 10000$ and known factorization of $p^n - 1$ could be computed over night.

Since the known $C_{p,n}(X)$ are still needed as explicit list it seems sensible to precompute and distribute all known $C'_{p,n}(X)$ in a similar way.

Keeping the known $C_{p,n}(X)$ as $C'_{p,n}(X)$ is necessary for backward compatibility: For example, it would be practically impossible to rewrite the character tables from the Modular Atlas in terms of another set of standard polynomials for finite fields.

We keep $C'_{p,4}(X) = C_{p,4}(X)$ because there is a quick algorithm to find these Conway polynomials (Bray).

Implementation

With an implementation in Magma all 24200 cases of $C'_{p,n}(X)$ with $p < 10000$ and known factorization of $p^n - 1$ could be computed over night.

Since the known $C_{p,n}(X)$ are still needed as explicit list it seems sensible to precompute and distribute all known $C'_{p,n}(X)$ in a similar way.

Keeping the known $C_{p,n}(X)$ as $C'_{p,n}(X)$ is necessary for backward compatibility: For example, it would be practically impossible to rewrite the character tables from the Modular Atlas in terms of another set of standard polynomials for finite fields.

We keep $C'_{p,4}(X) = C_{p,4}(X)$ because there is a quick algorithm to find these Conway polynomials (Bray).

Implementation

With an implementation in Magma all 24200 cases of $C'_{p,n}(X)$ with $p < 10000$ and known factorization of $p^n - 1$ could be computed over night.

Since the known $C_{p,n}(X)$ are still needed as explicit list it seems sensible to precompute and distribute all known $C'_{p,n}(X)$ in a similar way.

Keeping the known $C_{p,n}(X)$ as $C'_{p,n}(X)$ is necessary for backward compatibility: For example, it would be practically impossible to rewrite the character tables from the Modular Atlas in terms of another set of standard polynomials for finite fields.

We keep $C'_{p,4}(X) = C_{p,4}(X)$ because there is a quick algorithm to find these Conway polynomials (Bray).

Implementation

With an implementation in Magma all 24200 cases of $C'_{p,n}(X)$ with $p < 10000$ and known factorization of $p^n - 1$ could be computed over night.

Since the known $C_{p,n}(X)$ are still needed as explicit list it seems sensible to precompute and distribute all known $C'_{p,n}(X)$ in a similar way.

Keeping the known $C_{p,n}(X)$ as $C'_{p,n}(X)$ is necessary for backward compatibility: For example, it would be practically impossible to rewrite the character tables from the Modular Atlas in terms of another set of standard polynomials for finite fields.

We keep $C'_{p,4}(X) = C_{p,4}(X)$ because there is a quick algorithm to find these Conway polynomials (Bray).