$\mathrm{mod}\ 2$ における既約多項式の分類と証明

有限体 $\mathbb{F}_2$ 上のモニック多項式の厳密な判定と網羅リスト

第1部：証明と判定アルゴリズム

ステップ1：1次因数の排除（超強力フィルター）

多項式 $f(x)$ が既約であるための大前提は、1次因数を持たない（$\mathbb{F}_2$ 内に根を持たない）ことです。これにより以下の2条件が導かれます。

- **条件①：** $f(0) \neq 0 \pmod 2$
  $\Longrightarrow$ 定数項は必ず 1 でなければならない（定数項がないと x で括れてしまうため）。
- **条件②：** $f(1) \neq 0 \pmod 2$
  $\mathrm{mod}\ 2$ において $x = 1$ を代入すると、値は「存在する項の個数」そのものになる。
  $\Longrightarrow$ したがって、**全体の項数は必ず「奇数個」でなければならない**（偶数項だと和が 0 になり $x+1$ を因数に持つため）。

※2次式・3次式の場合は、1次因数を持たないことが証明できれば、自動的に既約が確定します。

ステップ2：2次因数の特定と合同式判定（4次・5次用）

4次以上の多項式の場合、1次因数がなくても「2次既約式」や「3次既約式」の積に分解される可能性があります。

ステップ1の条件を満たす2次式を調べると、x^2+x+1 **のただ1つ**しか存在しません。したがって、4次・5次式でステップ1を通過したものが可約であるとすれば、それは必ず x^2+x+1 を因数に持ちます。

多項式 x^2+x+1 による剰余環（$\mathbb{F}_2[x]/(x^2+x+1)$）を考えます。$x^2 \equiv x+1$ であり、$\mathrm{mod}\ 2$ では $-1 \equiv 1$ であるため、以下の強力な「次数下げ」ルールが得られます。

$$
\begin{aligned}
&x^2 \equiv x+1 \\
&x^3 \equiv x \cdot x^2 \equiv x(x+1) = x^2+x \equiv (x+1)+x = 2x+1 \equiv 1 \\
&x^4 \equiv x \cdot x^3 \equiv x \cdot 1 = x \\
&x^5 \equiv x \cdot x^4 \equiv x^2 \equiv x+1
\end{aligned}
$$

このルールを候補の多項式に適用し、**結果が 0 になれば可約、そうでなければ既約**であると厳密に証明できます。

第2部：5次多項式の具体的な計算過程

ステップ1のフィルター（定数項が1、項数が奇数）を突破した8個の候補式に対し、ステップ2の次数下げルールを適用して余りを求める詳細なプロセスです。（$\mathrm{mod}\ 2$ においれは $2=0, 3=1, 4=0$ となる点に注意して展開します）

【3項式のグループ（4個）】

① x^5+x^4+1

$$\begin{aligned} x^5+x^4+1 &\equiv (x+1)+x+1 \\ &= 2x+2 \\ &\equiv 0 \pmod 2 \quad \longrightarrow \text{可約} \end{aligned}$$

② x^5+x^3+1

$$\begin{aligned} x^5+x^3+1 &\equiv (x+1)+1+1 \\ &= x+3 \\ &\equiv x+1 \not\equiv 0 \pmod 2 \quad \longrightarrow \text{既約} \end{aligned}$$

③ x^5+x^2+1

$$\begin{aligned} x^5+x^2+1 &\equiv (x+1)+(x+1)+1 \\ &= 2x+3 \\ &\equiv 1 \not\equiv 0 \pmod 2 \quad \longrightarrow \text{既約} \end{aligned}$$

④ x^5+x+1

$$\begin{aligned} x^5+x+1 &\equiv (x+1)+x+1 \\ &= 2x+2 \\ &\equiv 0 \pmod 2 \quad \longrightarrow \text{可約} \end{aligned}$$

【5項式のグループ（4個）】

⑤ $x^5+x^4+x^3+x^2+1$

$$\begin{aligned} x^5+x^4+x^3+x^2+1 &\equiv (x+1)+x+1+(x+1)+1 \\ &= (x+x+x)+(1+1+1+1) \\ &= 3x+4 \\ &\equiv x \not\equiv 0 \pmod 2 \quad \longrightarrow \text{既約} \end{aligned}$$

⑥ $x^5+x^4+x^3+x+1$

$$
\begin{aligned}
x^5+x^4+x^3+x+1 &\equiv (x+1)+x+1+x+1 \\
&= (x+x+x)+(1+1+1) \\
&= 3x+3 \\
&\equiv x+1 \not\equiv 0 \pmod{2} \quad \longrightarrow \text{既約}
\end{aligned}
$$

⑦ $x^5+x^4+x^2+x+1$

$$
\begin{aligned}
x^5+x^4+x^2+x+1 &\equiv (x+1)+x+(x+1)+x+1 \\
&= (x+x+x+x)+(1+1+1) \\
&= 4x+3 \\
&\equiv 1 \not\equiv 0 \pmod{2} \quad \longrightarrow \text{既約}
\end{aligned}
$$

⑧ $x^5+x^3+x^2+x+1$

$$
\begin{aligned}
x^5+x^3+x^2+x+1 &\equiv (x+1)+1+(x+1)+x+1 \\
&= (x+x+x)+(1+1+1+1) \\
&= 3x+4 \\
&\equiv x \not\equiv 0 \pmod{2} \quad \longrightarrow \text{既約}
\end{aligned}
$$

第3部：各次数の分類リストサマリー（2次〜5次）

各次数 n における既約多項式の個数は、ガウスの公式 $N_2(n) = \frac{1}{n}\sum_{d|n}\mu(d)2^{n/d}$ と一致します。

次数	すべてのモニック多項式	根なしフィルター通過数	既約多項式の総数
2次	$2^2 = 4$ 個	1 個	**1 個**
3次	$2^3 = 8$ 個	2 個	**2 個**
4次	$2^4 = 16$ 個	4 個	**3 個**
5次	$2^5 = 32$ 個	8 個	**6 個**

■ 2次多項式（総数：1個）

定数項が 1 で、全体の項数が奇数（3項式）となる2次式は、以下の1個のみです。

x^2+x+1 **既約 (唯一の2次既約)**

■ 3次多項式（総数：2個）

定数項が 1 で項数が奇数（3項式）となるものは $\binom{2}{1} = 2$ 個です。3次式もフィルター通過時点で既約確定です。

$x^3 + x + 1$	既約 (1)
$x^3 + x^2 + 1$	既約 (2)

■ 4次多項式（総数：3個）

項数が奇数となるものは $\binom{3}{1} + \binom{3}{3} = 4$ 個。ここから、唯一の2次既約式の平方 $(x^2 + x + 1)^2 = x^4 + x^2 + 1$ を排除します。

$x^4 + x^3 + 1$ 既約 (1)	$x^4 + x + 1$ 既約 (2)	$x^4 + x^3 + x^2 + x + 1$ 既約 (3)

$x^4 + x^2 + 1$ 可約 ($(x^2 + x + 1)^2$)

■ 5次多項式（総数：6個）

第2部で計算した通り、3項式から2個、5項式から4個が生き残ります。

【3項式のグループ】

$x^5 + x^3 + 1$ 既約	$x^5 + x^2 + 1$ 既約	$x^5 + x^4 + 1$ 可約 ($(x^2 + x + 1)(x^3 + x^2 + 1)$)

$x^5 + x + 1$ 可約 ($(x^2 + x + 1)(x^3 + x + 1)$)

【5項式のグループ】

$x^5 + x^4 + x^3 + x^2 + 1$ 既約	$x^5 + x^4 + x^3 + x + 1$ 既約	$x^5 + x^4 + x^2 + x + 1$ 既約

$x^5 + x^3 + x^2 + x + 1$ 既約