AP SEIKO — スプリント数学 No.18

# 整数・合同式を"剰余の代数"で読む
# —— mod計算を武器として使いこなす

🎯 **今日のゴール：**

② 採点者が「理解している」と判断する答案の書き方を習得する

「余りを場合分けで調べる」高校の手法から脱皮し、 **合同式（mod）・フェルマーの小定理・中国剰余定理（CRT）** を使って 整数問題を代数的に処理できるようにする。RSA暗号の仕組みまで見渡す。

## 📌 この授業の問い

1. **$7^{100}$ を 5 で割った余りを、場合分けなしに mod で一瞬で求められるか？**
2. **フェルマーの小定理 $a^{p-1} \equiv 1 \pmod{p}$ はなぜ成り立つか？（p は素数・p∤a）**
3. **中国剰余定理（x≡2 mod 3 かつ x≡3 mod 5 の同時解）をどう構成するか？**

※ 高校：「余りを場合分けで地道に確認」 → 大学：「合同式の代数・フェルマー小定理・CRT で高速処理」

## 💡 合同式の代数的構造

**📐 合同式の基本性質**

$$a \equiv b \pmod{m} \iff m \mid (a-b)$$

足し算・掛け算が普通の等式と同じように使える——これが「mod の代数」の威力

**🔑 フェルマーの小定理（No.7の延長）** p が素数、p∤a のとき：$a^{p-1} \equiv 1 \pmod{p}$

→ 大きな指数の余りを「p − 1 で割った余りの指数」に還元できる

例：$7^{100}$ mod 5 → $7 \equiv 2 \pmod{5}$、$2^4 \equiv 1 \pmod{5}$（フェルマー） → 100=4×25 → $2^{100} \equiv 1^{25} \equiv$ **1**

採点者の視点

# 採点者はここを見ている —— 整数・剰余の代数の問題で合格答案はこういう「構造」をしている

## ① なぜ同じ答えでも評価が違うのか

清光学院の講師陣は、これまでに皆さんと同じ志を持った先輩受験生たちの答案を何千枚も採点し、合格・不合格の判定を下してきました。その経験から言えることが一つあります。

**「正しい答えを出していても、なぜそう考えたのかが見えない答案は、採点者の印象に残らない。」**

整数・剰余の代数の問題では、*mod計算の適用根拠*の理解が答案の質を大きく左右します。

## ② 整数・剰余の代数の問題で採点者が見ているポイント

「mod mで考えると乗法が保存されるから」と根拠を示す答案が採点者評価を上げる

> 💡 **この授業の使い方**
> 各問題のワンポイントには「採点者がどこを評価するか」の視点が含まれています。答えを出すだけでなく、根拠を一文添える習慣を意識しながら取り組んでください。

## ③ 総合型選抜・口頭試問でも同じ構造が問われる

採点者（大学教員）が口頭試問で確認したいのは「答えが出るか」ではなく「思考の構造を説明できるか」です。この授業で習得する「上から俯瞰する」視点は、あらゆる試験形式に通用します。

## 📚 続きは講義でご覧いただけます

この教材には、採点者の視点・核心的な解法・入試問題・演習・まとめがさらに収録されています。
大学教授陣が設計した「普通の授業では出会えない接続点」を体験できる完全版は講義でご提供いたします。