AP SEIKO ― スプリント数学 No.7

整数論の入口
―― 合同式で余りの問題を一瞬で処理する

🎯 **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
合同式（modular arithmetic）を道具として使いこなし、 **フェルマーの小定理・オイラーの定理・中国の剰余定理** まで到達する。余りの計算を「力ずく」から「代数的に一瞬で処理する」へ変換する。 RSA 暗号の仕組みまで接続。

📌 この授業の問い

1. **$a \equiv b \pmod m$ の定義を言えるか？加法・乗法・累乗に関してどう使うか？**
2. **フェルマーの小定理（$a^{p-1} \equiv 1 \pmod p$）を使って大きな累乗の余りを一瞬で求められるか？**
3. **中国の剰余定理（CRT）の主張と使い方を説明できるか？**

※ 高校：「余りを出す場合分け・帰納法」→ 大学：「合同式・フェルマーの小定理・CRT」

💡 高校解法 vs 大学解法の比較

問題	高校の解法	大学の解法（合同式）
n^3-n が 6 の倍数	連続3整数の積に分解・場合分け	$n^3 \equiv n \pmod 2$ かつ $n^3 \equiv n \pmod 3$ を合同式で示す
2^{100} を 7 で割った余り	$2^1=2, 2^2=4, 2^3=8 \equiv 1 \pmod 7$…の周期を手で計算	フェルマー：$2^6 \equiv 1 \pmod 7$、$100=6\times16+4 \to 2^{100} \equiv 2^4 \equiv 2 \pmod 7$
連立余り条件	具体的に書き出して確認	中国の剰余定理（CRT）で構成的に解く
RSA 暗号	扱わない	フェルマー・オイラーの定理で解読鍵の原理を説明

採点者の視点

採点者はここを見ている —— 整数論・合同式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。」

整数論・合同式の問題では、*合同式を使う根拠*の理解が答案の質を大きく左右します。

② 整数論・合同式の問題で採点者が見ているポイント

「mod nで考えると」と宣言してから計算する答案が採点者に明快と映る

> 💡 **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。