有限体と整数論

平泉 政宗 @hrizm (from 関東地方)

2012/03/31

初等整数論の中でも重要な定理である，**平方剰余の相互法則** (quadratic reciprocity law) と，その証明に用いる**有限体** (finite field) を紹介したいと思っています．「予備知識を仮定しない」と言ってしまった関係で，体の定義および $\mathbb{Z}/n\mathbb{Z}$ の構成から話をしていきますので，大学数学の知識はほとんど必要ないと思います (強いて言えば集合で使う言葉くらいです)．話の順序は，体の定義→有限体の構成→相互法則の紹介→計算例という流れです．平方剰余の相互法則と有限体の話を通して，初等整数論の雰囲気が味わえればと思います．

また，ゼロから平方剰余の相互法則まで寄り道せずに突き進んでいきたい関係で，少々不正確な表現，表記になっている部分が多々あります．その辺りを多少ご理解頂きたいですが，あまりにひどい場合は指摘して頂けると助かります．

【知っておくと話が簡単に聞こえることがら】

- 群，環，体の定義
- $\mathbb{Z}/n\mathbb{Z}$ の作り方，可換環であることの証明
- 算数 (特に掛け算，割り算)