所属： 高知工業高等専門学校 ソーシャルデザイン工学科

研究タイトル：マジックのようなフェルマーの小定理の証明

氏名：	高木和久 ／ TAKAGI Kazuhisa	E-mail：	ktakagi@ge.kochi-ct.ac.jp
職名：	准教授	学位：	理学修士（名古屋大学）
所属学会・協会：	日本数学教育学会，教育システム情報学会		

キーワード：	剰余系、フェルマーの小定理、ユークリッドの互除法、ウィルソンの定理
技術相談提供可能技術：	数学教育

研究内容： 中学生にも分かるように、剰余系を用いずにフェルマーの小定理を証明する

p枚のカードに数字 $0,1,\cdots,p-1$ が書かれていて、番号順に並んでいる。
例えば$p=5$のときは次のようになる。

$0 \rightarrow (0\ 1\ 2\ 3\ 4)$

先頭のカードを最後尾に持ってゆく操作を1 −シャッフルと名付ける。

$1 \rightarrow (1\ 2\ 3\ 4\ 0)$

1 −シャッフルをp回行うとp枚のカードは初期状態（0 1 2 3 4）に戻る。

最後尾のカードを先頭に持ってくる操作を逆1 −シャッフルと呼ぶ。逆1 −シャッフルは負の数を用いて次のように表すことができる。

$-1 \rightarrow (4\ 0\ 1\ 2\ 3)$

この数字の並びは4 −シャッフルを行った結果と同じである。このことを記号で

$-1 \equiv 4$

と表すことにする。一般に、逆k −シャッフルを行った結果は$(p-k)$ −シャッフルを行った結果と一致する。

さて、pが素数の時フェルマーの小定理が成り立つ。ここでは$p=5$の場合を証明する。

$x^{p-1}-1=x^4-1=(x^2-1)(x^2+1)=(x+1)(x-1)(x^2+1)$

である。1 −シャッフルは逆4 −シャッフルと同じなので

$x+1 \equiv x-4\,, x^2+1 \equiv x^2-4$

が成り立つから

$x^4-1 \equiv (x-4)(x-1)(x^2-4) \equiv (x-4)(x-1)(x+2)(x-2)$

更に、2 −シャッフルは逆3 −シャッフルと同じだから

$x^4-1 \equiv (x-4)(x-1)(x-3)(x-2) \equiv (x-1)(x-2)(x-3)(x-4)$

この式より、$x=1,2,3,4$ のとき

$x^4-1 \equiv 0$

が成り立つ。（フェルマーの小定理）

なお、この方法でユークリッドの互除法を行ったり、ウィルソンの定理

pが素数 $\leftrightarrow (p-1)! \equiv -1$

を剰余系を用いずに証明することができる。