フェルマーの小定理

Joh @物理のかぎプロジェクト

2006-04-23

群論を整数論に応用して得られる一つの結果として，フェルマーの小定理を見ます．フェルマーの小定理は群論を使わなくても証明できますが，ここまでに勉強した群論の知識を使うと，非常にエレガントに証明できてしまいます．

図 1　(フランスの切手にもなっているフェルマー)

フェルマーの小定理

整数全体 Z の整数 n の剰余類のうち，0 を含む剰余類を除いた集合 ${Z_n}^*$ を考えます．このとき，n を素数 (以後 p と書きます) とすると，p は約数を持ちませんから，${Z_n}^*$ は p の剰余類によって次のように書けます．

$$ {Z_n}^* = \{[1], [2], ..., [p-1]\} $$

よって，位数は $p-1$ です．

$$ |{Z_n}^*| = p - 1 $$

*1 『3 以上の整数 n に対し $x^n + y^n = z^n$ を満たす整数 x, y, z の組は存在しない』という有名なフェルマーの定理と区別するために，こちらの方はフェルマーの小定理と呼ばれます．有名な方は『フェルマーの大定理』もしくは『フェルマーの最終定理』などと呼ばれます．フェルマーの大定理は，長年に渡って証明不可能だと思われていましたが，1995 年にワイルズ (Andrew John Wiles(1953-)) によって証明されたのは，まだ記憶に新しいところです．歴史上，数多くの数学者がフェルマーの大定理を解決しようと試み，証明にこそ失敗しましたが，その過程で到達した様々な結果や概念によって代数学は大きな進歩を遂げました．さて，私達が勉強するのは小定理の方です．

これがフェルマーの小定理です．簡単でしたね！ただし，整数論の教科書に出てくるのは，次の形です．ここまでの議論は，次の定理の証明になっています．

theorem

整数 a を，p の倍数ではない整数とし，p を素数とするとき，$a^{p-1} \equiv 1 \ (\mathrm{mod}.p)$ がなりたつ．

この定理で何が分かるのか，ちょっと分かり難いかも知れません．例を考えてみれば，なかなか強力な定理だということが分かると思います．

例： 218^{23} を 23 で割った余りを求めてください．

フェルマーの小定理より，$218^{23} = 218 \times (218^{23-1}) \equiv 218 \equiv 11 \ (\mathrm{mod}.23)$ となって，余り 11 が瞬時に求まります．

系

フェルマーの小定理を，群論で使いやすい表現に書き直すと次のようになります．

theorem

群 ${Z_p}^*$ で p が素数のとき，$|{Z_p}^*| = p - 1$ がなりたつ．

さらに発展形として，次の定理を考えます．

theorem

群 ${Z_n}^*$ の位数が素数 p の冪 p^k のとき，$|{Z_n}^*| = p^k\left(1 - \frac{1}{p}\right)$ がなりたつ．

proof

この場合，1 と p^k の間にある，p^k と互いに素であるような数は，1 から p^k の間にある数のうち，p の倍数，$p, 2p, 3p, ..., p^k - 2p, p^k - p, p^k$ を除いたものです．このような数は，全部で p^{k-1} 個ありますので，1 と p^k の間にある，p^k と互いに素である整数は全部で $p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$ 個あると言えます．よって $|{Z_n}^*| = p^k\left(1 - \frac{1}{p}\right)$ がなりたちます．■

さらに一般の場合には，次のように定理を拡張できます．

theorem

群 ${Z_n}^*$ の位数 n が $n = {p_1}^{k_1}{p_2}^{k_2} \cdots {p_s}^{k_s}$ のように素因数分解できるとき，$|{Z_n}^*| = {p_1}^{k_1}{p_2}^{k_2} \cdots {p_s}^{k_s}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right)$ がなりたつ．

*2 フェルマーの小定理をつかえば，このように，とんでもなく大きな数でも，一瞬で余りが分かってしまいます．素数の判定や暗号理論に欠かせない定理なのです．

この定理の証明は省略します．これは，このあとに勉強する シローの定理 の一つの表現になっています．