高校生のための現代数学講座
「数論と暗号」
講義 (1)　織田　孝幸

東京大学
玉原国際セミナーハウス
2005 年 9 月 10 日

「大きな素数」

本日の話の目標は次の 3 つとする.
(1) 素数は無限にたくさんあることを証明する.
いくつかある標準的な証明では、具体的にどんどん大きな素数を作っていく方法が分からない. エラトステネスのふるいでは、大きくなるにつれて「紙の無駄」が増える. そこで
(2) 大きな素数の作り方として定評のあるメルセンス数（2^p-1 の形の素数）に関して簡単に知る. 3 番目に、時間があれば、
(3) 未解決の有名な問題の Goldbach 予想について触れる.

1. 素数は無限にある

1.1 Euclid の証明、2 千年以上前の世界最初の証明

定理 無限に多くの素数が存在する.

証明　$p_1=2<p_2=3<\cdots<p_r$ を素数の全てだと仮定する. $N=p_1p_2\cdots p_r+1$ とおいて、p を N を割り切る素数であるとする. すると p は $p_1,p_2,\cdots,p_r$ のどれかではありえない. どれかに等しいとすると、p は差 $N-p_1p_2\cdots p_r=1$ も割り切ることになるが、それは不可能である. したがって、この p は新しい素数であり、$p_1,p_2,\cdots,p_r$ が素数のすべてであるという仮定に矛盾する.

1.2 Kummer の別証明

証明　有限個の素数 $p_1=2<p_2=3<\cdots<p_r$ しかないと仮定する. $P=p_1p_2\cdots p_r>2$ と置く. 整数 $P-1$ は素数の積なので、P の共通の約数 p_i をもつ. すると p_i は $P-(P-1)=1$ を割り切ることになり、これは不合理である.

1.3 Goldbach の別証明

補題 Fermat 数 $F_n=2^{2^n}+1$ は 2 個ずつ互いに素である.

証明　帰納法により $F_m-2=F_0F_1\cdots F_{m-1}$ を示すのはやさしい. このことから、d が F_n と F_m の両方 $(n<m)$ を割り切るならば、d は F_m-2 を割り切ることが分かる. よって d は 2 を割り切る. しかしすべての Fermat 数は奇数だから、d は 1 に等しい.

定理 無限に多くの素数が存在する.

証明　各 Fermat 数 F_n に対して、その素因数 p_n を選ぶ. 補題により、これらはすべて相異なる素数である. つまり、無限に多くの素数が存在する.

注 定義より $F_{m+1}-1=(F_m-1)^2$ あるいは同じことであるが、$F_{m+1}-2=(F_m-2)F_m$ が成立する. これより $F_m-2=F_0F_1\cdots F_{m-1}$ を示す.

2. Mersenne 素数

定義 2^n-1 の形の素数をメルセンヌ素数という.

命題 正の整数 n に対し 2^n-1 が素数であれば、n も素数である.

メルセンヌ素数に限らず、ある数 n が与えられたとき、それが素数かどうかなるべく短時間に判定する方法が必要になる. 最もよく知られているのは、次の Fermat の小定理を使う判定法 (Fermat Test) である.

Fermat の小定理 n が素数であるとき、n と互いに素な数 a に対して、合同式 $a^{n-1} \equiv 1 \pmod{n}$ が成立する.

フェルマーの定理は、与えられた a に対し、n が素数である必要条件を与えるが十分条件ではない. ($a=1$ のときを考えよ).

ある $a>1$ に対して、$a^{n-1} \equiv 1 \pmod{n}$ であるとき、n は概素数という. 多くの場合素数であるからである. n が概素数で、本当の素数でないとき、擬素数という.

メルセンヌ素数専用の素数性の判定条件 (Lucas-Lehmer の定理) がある.

Lucas-Lehmer 判定法 (1930 年) 奇数 n に対してメルセンヌ数 $M(n)=2^n-1$ が素数であるのは、

$$S_{n-1} \equiv 0 \pmod{M(n)}$$

であるときで、そのときに限る. ここで $S_0=4,\ S_{k+1}=S_k^2-2$ である.

3. Goldbach の問題

Goldbach が 1742 年に Euler に書いた手紙が発端になった予想である. 整理した形では次のように述べられる.

Goldbach 予想 6 以上の任意の偶数は、二つの素数の和として表される.

1998 年現在、計算機では 14 桁 15 桁くらいまで確認されているようである. 理論的な研究は、1966 年に Chen が、十分大きな偶数は、素数と P_2（せいぜい二つの素因数をもつ数）の和で表わされることが分かっている.

奇数 Goldbach 予想 9 以上の任意の奇数は、三つの素数の和として表される.

現時点では、奇数が $n>10^{43000}$ ならば正しいことが証明されている. 十分大きな素数に対して、奇数 Goldbach 予想が正しいことを示したのは、ロシアの Vinogradov という数学者が 1937 年にやった. その後の改良で、n が 43000 桁以下で確認すればよいことになったわけである. これでも現在の計算機でもしらみつぶしで確認できるには大きすぎる.

文献

[1] 素数大百科、Chris K. Caldwell 編著、SOJIN 編訳、共立出版、2004 年 2 月
[2] その他、リベンボイム (Ribenboim、カナダの Queen 大学名誉教授) の本 (多くは吾郷さんの翻訳)