第1章　序

1.1　ピタゴラス方程式

ピタゴラスの定理（三平方の定理）は古くから知られている．

定理 1.1 直角３角形の直角をはさむ２辺の長さを a, b とし，他の１辺の長さを c とすれば，

$$a^2 + b^2 = c^2$$

が成り立つ．

長さが整数または有理数である直角３角形を見つけることは，方程式

$$x^2 + y^2 = z^2$$

の自然数解を求めることに帰着する． このように自然数や整数，または有理数の解に着目する場合，上記方程式は**ピタゴラス方程式**と呼ばれる． 次の定理も古くから知られていたようである．

定理 1.2 ピタゴラス方程式

$$x^2 + y^2 = z^2$$

の自然数解は，$u > v$ をみたす自然数 u, v をとって

$$(x, y, z) = (u^2 - v^2,\ 2uv,\ u^2 + v^2) \quad \text{または} \quad (2uv,\ u^2 - v^2,\ u^2 + v^2)$$

とおくことによりすべて得られる．

たとえば，$u = 2, v = 1$ あるいは $u = 3, v = 2$ とすれば，

$$(x, y, z) = (2^2 - 1^2, 2 \cdot 2 \cdot 1, 2^2 + 1^2) = (3, 4, 5)$$
$$(x, y, z) = (3^2 - 2^2, 2 \cdot 3 \cdot 2, 3^2 + 2^2) = (5, 12, 13)$$

というよく知られた解が得られるし，$u = 2012, v = 927$ をとれば，

$$(x, y, z) = (3188815, 3730248, 4907473)$$

というあまり知られていない（っていうかほとんど誰も知らない）解も出てくる． 定理の証明は講義で行う予定である．

1.2　フェルマーの最終定理

ピタゴラス方程式は 2 次式で表されているが，これを 3 次にするとどうなるか？ フェルマー（17 世紀の人）は，そのような方程式には自然数解がなく，さらに 4 次以上でも同様に自然数解がないと述べている． さらに，ある本の余白に,「その『驚くべき証明』を発見したがそれを記すにはこの余白は狭すぎる」と書き残した． 現在まで彼の証明は見つかっていない．

定理 1.3 (フェルマーの最終定理) 自然数 $n \geq 3$ に対して，方程式

$$x^n + y^n = z^n$$

は自然数解をもたない．

この定理は，長い間証明が知られていなかったので，かつては『フェルマー予想』とも呼ばれ，整数論における難問のひとつであった． フェルマー自身によって $n = 4$ の場合が証明され，$n = 3$ に対してはオイラーが証明を与えている（それぞれ，17, 18 世紀）． その後，ソフィー・ジェルマン，ディリクレ，クンマー等の貢献により，19 世紀中に 100 までのすべての n に対して正しいことが確かめられたが，20 世紀になって整数論や代数幾何学の理論が少しずつ整えられた結果，1994 年ワイルズによって完全な証明が与えられた．その証明は数多くの高度な理論を駆使して構成され，大胆な発想に満ちているが，その概略の一部でも紹介するだけの余白はここにはない．

1.3　ABC 予想

フェルマーの最終定理と関連して，次に述べる ABC 予想 がある． 互いに素な自然数 a, b に対して，$a + b = c$ をみたす組 (a, b, c) を abc-トリプルという． また，自然数 m に対してその素因数の重複を許さない積を $\mathrm{rad}(m)$ で表わす． たとえば，$\mathrm{rad}(10) = 2 \cdot 5 = 10$, $\mathrm{rad}(45) = 3 \cdot 5 = 15$, $\mathrm{rad}(1024) = 2$. ABC 予想は，ほとんどの abc-トリプル (a, b, c) に対して，$\mathrm{rad}(abc)$ は本質的に c より小さくはなり得ないことを主張する． 正確には以下ように定式化される．

予想 1.4 (ABC 予想 [I]) 任意の $\varepsilon > 0$ に対して，

$$\mathrm{rad}(abc)^{1+\varepsilon} < c$$

をみたす abc-トリプル (a, b, c) は有限個しか存在しないであろう．

とくに $\varepsilon = 1$ の場合，上記不等式をみたす abc-トリプルは（等号を付けても）存在しないと期待されており，それを ABC 予想と呼ぶこともある．

予想 1.5 (ABC 予想 [II]) すべての abc-トリプル (a,b,c) に対して，

$$\mathrm{rad}(abc)^2 > c$$

が成り立つであろう．

ABC 予想の簡単な帰結としてフェルマーの最終定理が導かれる．すなわち，予想 1.5 が正しければ，任意の $n \geq 3$ に対して $x^n + y^n = z^n$ の自然数解は存在しないことが初等的に導かれる．実際，もし解 x, y, z が存在すれば，予想 1.5 より

$$z^n < \mathrm{rad}(x^n y^n z^n)^2$$

であるが，$x < z,\ y < z$ かつ $\mathrm{rad}(x^n y^n z^n) = \mathrm{rad}(xyz) \leq xyz$ から

$$(xyz)^n < z^{3n} < \mathrm{rad}(x^n y^n z^n)^6 \leq (xyz)^6$$

すなわち，$n = 3, 4, 5$ を得るが，この場合はすでに解がないことが初等的にわかっているので矛盾である．予想 1.4 からは，解が存在しても有限個であることが導かれる．各自確かめてみよ．なお，各 $n \geq 3$ について，それぞれ有限個しか解がないことは以前から知られていた（ファルティングスの定理 (1983)）．それよりも強く，すべての $n \geq 3$ にわたって，解は有限個しかないことが ABC 予想（予想 1.4）から導かれるわけである．

この９月，ABC 予想が肯定的に解決されたという情報がもたらされた．ABC 予想はきわめて広い応用をもつことが知られており，上記のフェルマーの最終定理を含めこれまで難解だった証明の簡略化や，多くの未解決問題の解決に寄与することが期待されている．それだけに，このニュースは衝撃的である．

1.4　有名な問題

一般に数学の問題は難しい概念を用いて語られ，専門に学んだ人でなければ問題を理解することすら困難であることが多い．しかし，整数論の問題は初等的に表現されるものもあり，それらの多くは中高生でも（もしかすると小学生でも）理解できる．ただし，問題が初等的に表現されるからといって，必ずしも初等的に解けるとはいえず，未解決のまま残ることも往々にしてある．前述の『フェルマーの最終定理（フェルマー予想）』も 20 年前まではそんな類の問題であった．他にもいくつかあるので思いつくままに列挙してみる．

素数が無限個存在することは古代から知られているが，次の定理は，初項と公比が互いに素な数列上にも素数が無限に現れることを示している．

定理 1.6 (ディリクレ) 互いに素な整数 a, b（ただし $a > 0$）に対して $an + b$ $(n \in \boldsymbol{N})$ の形の素数が無限に存在する．

すなわち，係数が互いに素な１次式に自然数を代入していけば，素数が無数に現れる．それでは，２次以上の場合はどうか？ ２次以上の整数係数の多項式（最高次係数は正）$f(x)$

に，自然数を代入していくと，$f(1), f(2), f(3), \cdots$ の中に素数が無限に現れるだろうか？現在までにそのような多項式 $f(x)$ はひとつも確認されていない．もっとも簡単なケースとして次の予想がある．

予想 1.7 n^2+1 $(n \in \boldsymbol{N})$ の形の素数が無数に存在するであろう．

この他に，素数に関する 2 つの有名な予想について述べる．

差が 2 である素数のペアを**双子素数**という．$(3,5),(5,7)$ はもっとも簡単な例であるが，計算を続けていくといくらでも大きなペアが見つかる，たとえば $(1698377, 1698379)$ など．

予想 1.8 (双子素数予想) 双子素数は無限組存在するであろう．

18 世紀半ば，ゴールドバッハはオイラーに宛てた手紙の中で，6 以上のすべての自然数は三つの素数の和で書けるだろう，という予想を述べた．偶数をそのような和で表せば素数のうち一つは 2 になっているはずだから，この予想は次のように述べることができる．

予想 1.9 (ゴールドバッハ予想) 6 以上の任意の偶数は二つの素数の和として表すことができるであろう．

これらの予想は，部分的な結果はあるものの，完全な解決にはほど遠いというのが現状である．現在では，コンピュータによる探索が進んでいて，かなり大きな自然数に対して予想の内容が正しいことが確かめらている（各自ググってみよ）．

その数より小さい約数の和がその数になるとき**完全数**という．たとえば，28 はその約数 $1,2,4,7,14$ の和と等しいので完全数である．2^n-1 が素数のとき $2^{n-1}(2^n-1)$ が完全数となることは古代から知られていた．さらにオイラーによって，偶数の完全数は必ずこのように表されることも証明されている．

予想 1.10 偶数の完全数は無限に存在するであろう．

この予想は，2^n-1 の形の素数が無数にあるだろう ということと同じである．このような素数は**メルセンヌ素数**と呼ばれ，現在 (2012 年 9 月) までに 47 個しか見つかっていない．一方，奇数の完全数は一つも発見されていない．

予想 1.11 奇数の完全数は存在しないであろう．

もし存在すれば 10^{300} より大きいことが示されているが，もちろんこれで予想が確認できたわけではない．

最後に述べる次の定理は，“カタラン予想” とよばれていたもので，ミハイレスクによって 2002 年に証明された．

定理 1.12 (カタラン予想) $x^m - y^n = 1$ をみたす 1 より大きい自然数 x, m, y, n の組は $(x,m,y,n) = (3,2,2,3)$ のみである．

前世紀までは難問中の難問のひとつと思われていたが，ミハイレスクは代数的整数論のオーソドックスな手法を用いて解決した．なお，この定理も，ABC 予想（予想 1.5）から比較的容易に導くことができる．