余りの世界と不定方程式

植松 哲也

名城大学 理工学部 数学科

August 4, 2017. 10:00〜12:00
総合数理プログラム夏季セミナー
@ 名城大学天白キャンパス H201

今日のお話：整数問題の図形的アプローチ

$\mathbb{F}_p$ において, 不定方程式
$x^2 + y^2 = 1$
の解はいくつある？ (第 3 部)

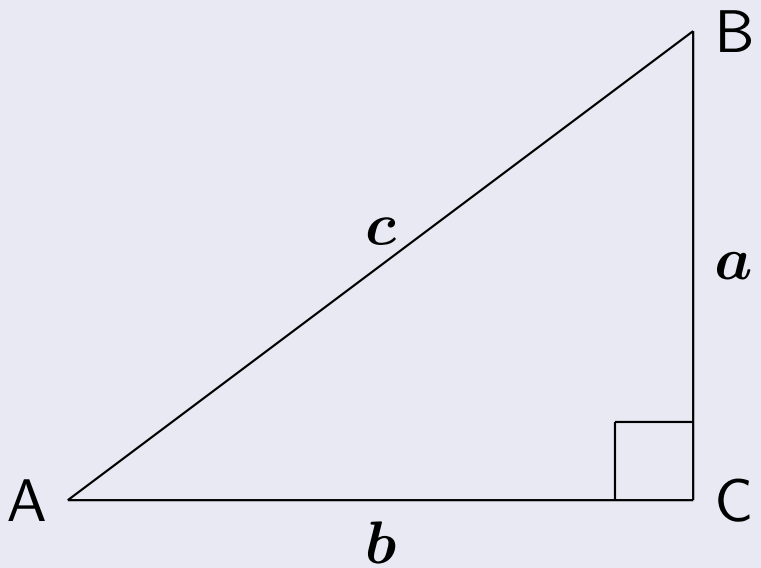
円 $x^2 + y^2 = 1$
の有理点
ピタゴラス数 (第 1 部)

素数 p で割った
余りの世界 $\mathbb{F}_p$ (第 2 部)

ピタゴラス数

ピタゴラスの定理 (三平方の定理)

$\angle \mathbf{C} = \mathbf{90}^\circ$ の直角三角形 $\mathbf{ABC}$ において, $a^2 + b^2 = c^2$ が成り立つ.



ピタゴラス数

ピタゴラス数

自然数の 3 つ組 (a, b, c) で, c を斜辺とする直角三角形の 3 辺の長さになっているものをピタゴラス数という：

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

Example

- $(3, 4, 5)$ はピタゴラス数.
- $(1, \sqrt{3}, 2)$ はピタゴラス数ではない. (無理数はダメ)
- $(-1, 1, \sqrt{2})$ もピタゴラス数ではない. (負の数もダメ)

Quiz 1

ピタゴラス数を思いつくままに挙げてみよう.
テーブルごとに書き出してみてください.

ピタゴラス数

答え合わせ

- $(3,4,5), (6,8,10), \cdots, (4,3,5)$
- $(5,12,13), (10,24,26), \cdots$
- $(7,24,25), (14,48,50), \cdots$
- 他に見つかった人・・・？
- $(55,48,73), (280,351,449)$ などもピタゴラス数！

$$55^2 + 48^2 = 3025 + 2304 = 5329 = 73^2.$$

$$280^2 + 351^2 = 78400 + 123201 = 201601 = 449^2.$$

- 私はどうやって見つけたでしょう？
  天から降ってきた, 手計算で頑張った, コンピュータに計算させた, ...

ピタゴラス数

Quiz 2

(合同, 相似なものは除いて) ピタゴラス数はいくつあるだろうか？

1. **100** 個より少ない.
2. **201784** 個.
3. 無数に存在する.

答え合わせ

3 無数に存在する.

実は, いくらでもピタゴラス数を作り出せる公式がある！

- 以下では, そのピタゴラス数公式を導いていきます.
- そのなかで, xy 平面上の直線や円の交点といった図形的な視点が活躍します.

ピタゴラス数

自然数から有理数へ

- $a^2 + b^2 = c^2$ となる自然数 (a, b, c) を見つけたい.
- 両辺を c^2 で割ると,

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$$

となるので, ピタゴラス数を見つけるには, 2 つの未知数を含む方程式

$$x^2 + y^2 = 1$$

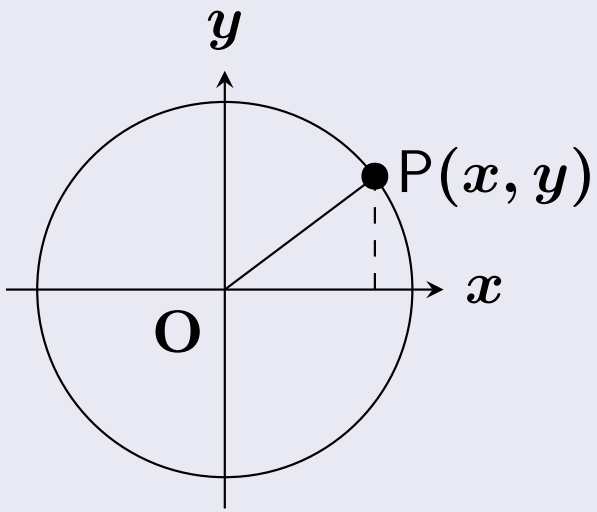
の有理数の解を見つければよい.

- 例. $\left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1$, $\left(\frac{12}{13}\right)^2 + \left(\frac{5}{13}\right)^2 = 1$
(このように未知数が 2 つ, 式が 1 つ, という方程式は, 解が一つに定まらないことが多く, 不定方程式 と呼ばれる.)

ピタゴラス数

円の方程式

- 原点 $\mathbf{O}(0,0)$ を中心とし, 半径 1 の円周上にある点 $\mathbf{P}(x,y)$ はどんな式を満たすだろうか？



- 原点 $\mathbf{O}$ と $\mathbf{P}$ の距離はピタゴラスの定理から,

$$\sqrt{(x-0)^2+(y-0)^2}$$

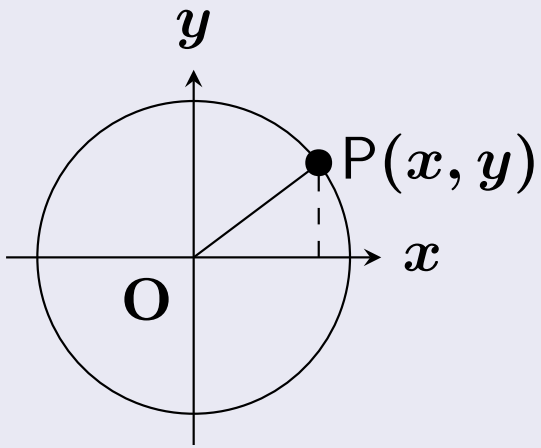
である. これが円の半径 1 に等しいので...

ピタゴラス数

円の方程式

- 原点中心, 半径 1 の円周上の点 (x, y) は次の方程式を満たす：

$$x^2 + y^2 = 1$$



- したがって, ピタゴラス数を見つける問題は,

  円 $x^2 + y^2 = 1$ の上に, x 座標も y 座標も有理数であるような点 (有理点) を見つけること

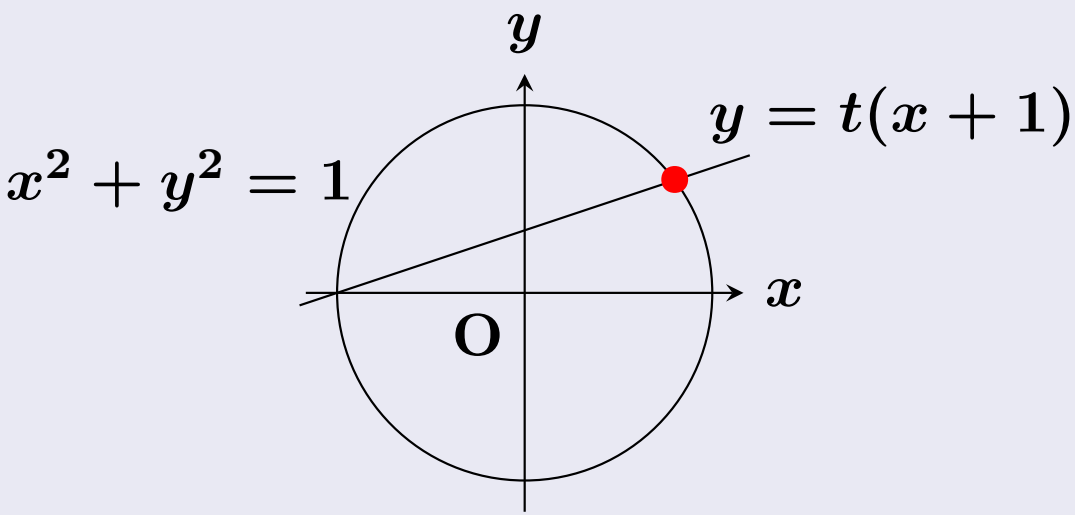
  と言いかえることができる.

直線と円の交点

- 点 $(-1, 0)$ を通り, 傾き t の直線の式は

$$y = t(x + 1).$$

- この直線と, 円 $x^2 + y^2 = 1$ の ($(-1, 0)$ 以外の) 交点を考えよう.



ピタゴラス数

直線と円の交点

- 交点の座標を求めるには, 連立方程式

$$\begin{cases} y = t(x+1) \\ x^2 + y^2 = 1 \end{cases}$$

を解けばよい.

- y を消去すると, x の 2 次方程式

$$(1+t^2)x^2 + 2t^2x + (t^2-1) = 0$$

が得られる.

ピタゴラス数

直線と円の交点

- 因数分解 (たすきがけ) すると,

$$\{(1+t^2)x+(t^2-1)\}(x+1)=0$$

となるので, 交点の x 座標は

$$x=-1,\quad \frac{1-t^2}{1+t^2}.$$

- $x=-1$ は調べたいものではないので, 交点の座標は

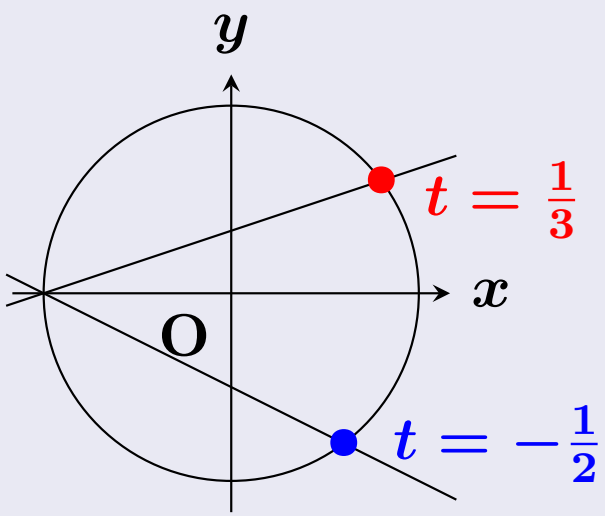
$$\left(\frac{1-t^2}{1+t^2},\frac{2t}{1+t^2}\right)$$

となる.

ピタゴラス数

円 $x^2+y^2=1$ 上の有理点

- 傾き t が有理数であれば, 交点の座標 $\left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right)$ の x 座標, y 座標もまた有理数となる.
- つまり, 有理数 t をひとつ決めると, 円 $x^2+y^2=1$ 上の有理点をひとつ作ることができる！ (しかも, 図から明らかに, 傾きが異なれば, 作られる有理点も違うものになる)



ピタゴラス数

公式の導出

- 交点の座標を利用して, ピタゴラス数を作り出す公式を求めよう. いま, 交点は $x^2 + y^2 = 1$ の上にあるので,

$$\left(\frac{1-t^2}{1+t^2}\right)^2 + \left(\frac{2t}{1+t^2}\right)^2 = 1$$

が成り立っている. 両辺を $(1+t^2)^2$ 倍すると,

$$(1-t^2)^2 + (2t)^2 = (1+t^2)^2$$

となる.

- $(1-t^2, 2t, 1+t^2)$ は自然数の 3 つ組ではないので, このままではピタゴラス数にならない.

ピタゴラス数

公式の導出

- そこで, 自然数 n, m (ただし, $n > m$) を用いて, $t = \dfrac{m}{n}$ を代入すると,

$$\left(1 - \frac{m^2}{n^2}, 2\frac{m}{n}, 1 + \frac{m^2}{n^2}\right)$$

となる. すべての座標を n^2 倍して, 形は変えずに, 辺の長さを自然数にしてやると...

まとめ (ピタゴラス数を作り出す公式)

n, m を (最大公約数が 1 の) 自然数とし, $n > m$ とする. このとき,

$$(n^2 - m^2, 2mn, n^2 + m^2)$$

はピタゴラス数になる. また, 相似なものを除けば, すべてのピタゴラス数はここから作り出すことができる！

ピタゴラス数

まとめ (ピタゴラス数を作り出す公式)

$$(n^2 - m^2, 2mn, n^2 + m^2) \quad (n > m)$$

Example

- $n = 8, m = 3$ としてみると,

$$(n^2 - m^2, 2mn, n^2 + m^2) = (55, 48, 73)$$

- $n = 20, m = 7$ としてみると,

$$(n^2 - m^2, 2mn, n^2 + m^2) = (351, 280, 449)$$

- 最大公約数が 1 であるような n と m の選び方は無数にあるので, ピタゴラス数も無数に存在することがわかる！ (Quiz 2 の答え)
- いろいろな数を代入して, ピタゴラス数を作ってみよう！

余りの世界

素数

2 以上の自然数で, 1 と自分自身以外に約数を持たない数. 小さい方から

$$\mathbf{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \cdots}$$

合同

- 素数 $\boldsymbol{p}$ をひとつ決める.
- 2 つの整数 $\boldsymbol{n, m}$ について, $\boldsymbol{n}$ を $\boldsymbol{p}$ で割った余りと, $\boldsymbol{m}$ を $\boldsymbol{p}$ で割った余りが等しい (つまり, $\boldsymbol{n - m}$ が $\boldsymbol{p}$ の倍数である) とき,

$$\overline{\boldsymbol{n}} = \overline{\boldsymbol{m}}$$

と書き, $\boldsymbol{n}$ と $\boldsymbol{m}$ は $\boldsymbol{p}$ を法として合同である, という.
数式で表すときに $\boldsymbol{p}$ を明示したいときは

$$\boldsymbol{n \equiv m \mod p}$$

と書くこともある.

余りの世界

Example

- $p = 5$ とする.

$$\overline{3} = \overline{8} = \overline{-2} = \overline{-17} = \cdots$$

$$\overline{-4} = \overline{1} = \overline{1001} = \cdots$$

- $p = 13$ とする.

$$\overline{97} = \overline{-20} = \overline{6} = \cdots$$

Quiz 3

$p = 7$ とする.
$\overline{-47}$, $\overline{111}$ はそれぞれ $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$ のどれと等しいか？

答え合わせ

- $-47 = (-7) \times 7 + 2$ だから, $\overline{-47} = \overline{2}$.
- $111 = 15 \times 7 + 6$ だから, $\overline{111} = \overline{6}$.

余りの世界

p 元体 $\mathbb{F}_p$

- 素数 p をひとつ決める.
- p で割った余りは, $0, 1, 2, \ldots, p-1$ の p 個だけ.
- 言いかえれば, どんな $\overline{n}$ も $\overline{0}$ から $\overline{p-1}$ のどれか1つと等しくなる.
- この, p で割った余りだけを集めてきた集合

$$\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\}$$

を $\mathbb{F}_p$ と書き, p 元体とよぶ.

Example

- $\mathbb{F}_2 = \{\overline{0}, \overline{1}\}$
- $\mathbb{F}_{11} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}\}$

余りの世界

$\mathbb{F}_p$ での足し算・引き算・掛け算・割り算

この p 個の「数」からなる世界 $\mathbb{F}_p$ でも，普通の有理数や実数のように，足し算・引き算・掛け算・割り算を考えることができる．計算の仕方は次のようにする．

Example ($p = 5$ のとき)

- $\overline{3} + \overline{4} = \overline{3+4} = \overline{7} = \overline{2}$.
- $\overline{1} - \overline{3} = \overline{1-3} = \overline{-2} = \overline{3}$.
- $\overline{3} \times \overline{2} = \overline{3 \times 2} = \overline{6} = \overline{1}$.　(つまり，$\overline{2}$ は $\overline{3}$ の逆数！　)
- $\overline{2} \div \overline{3} = \overline{12} \div \overline{3} = \overline{12 \div 3} = \overline{4}$.
  「$\overline{3}$ で割る」ということは，「$\overline{3}$ の逆数を掛ける」ことだと考えて，

$$\overline{2} \div \overline{3} = \overline{2} \times \overline{2} = \overline{4}$$

  と考えてもよい．

発展的なお話

- $\overline{2} \div \overline{3} = \overline{12} \div \overline{3} = \overline{12 \div 3} = \overline{4}$.
- 2 が 3 で割り切れないので, 2 と合同で, しかも 3 で割り切れる 12 に取り替えて割り算をしたが, 12 の代わりに -3 や 27 を取ってくる人もいるかもしれない. こうやっても

$$\overline{-3} \div \overline{3} = \overline{-3 \div 3} = \overline{-1} = \overline{4}$$

となって, 結局同じ値になる. あるいは, 割る数 $\overline{3}$ の方を $\overline{-2}$ として,

$$\overline{2} \div \overline{-2} = \overline{2 \div (-2)} = \overline{-1} = \overline{4}$$

と考える人もいるだろう.
このような, 合同な数の取り替え方によらずに, いつでもちゃんと同じ答えが出てくるかどうかということを本当は議論する必要がある.

余りの世界

演算表

この余りの世界に慣れていない人にとっては, 計算が大変なので, (足し算と) 掛け算の「九九の表」に当たるものを作っておくと便利である. これを演算表という.

Example ($p = 5$ のとき)

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

- $\overline{3} \div \overline{4} = \overline{3} \times \overline{4} = \overline{12} = \overline{2}$
  ($\overline{4}$ の行を見て, $\overline{1}$ があるのは $\overline{4}$ の列だから, $\overline{4}$ の逆数は $\overline{4}$ とわかる.)

余りの世界

Quiz 4

- $\mathbb{F}_7$ の掛け算の演算表を完成させよ. ($\overline{\bullet}$ を省略しています.)

$\times$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{4}$	$\mathbf{5}$	$\mathbf{6}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$		$\mathbf{3}$			
$\mathbf{2}$	$\mathbf{0}$			$\mathbf{6}$		$\mathbf{3}$	
$\mathbf{3}$	$\mathbf{0}$	$\mathbf{3}$	$\mathbf{6}$				$\mathbf{4}$
$\mathbf{4}$	$\mathbf{0}$				$\mathbf{2}$		$\mathbf{3}$
$\mathbf{5}$	$\mathbf{0}$	$\mathbf{5}$		$\mathbf{1}$		$\mathbf{4}$	
$\mathbf{6}$	$\mathbf{0}$	$\mathbf{6}$	$\mathbf{5}$	$\mathbf{4}$			

- $\mathbb{F}_7$ で $\overline{\mathbf{2}} \div \overline{\mathbf{3}}$ を計算しなさい.
- $\mathbb{F}_7$ で方程式 $\overline{\mathbf{5}}\boldsymbol{x} + \overline{\mathbf{4}} = -\boldsymbol{x} + \overline{\mathbf{1}}$ を解け.
- $\mathbb{F}_7$ で方程式 $\boldsymbol{x}^{\mathbf{2}} + \boldsymbol{x} + \overline{\mathbf{1}} = \overline{\mathbf{0}}$ を解け.

余りの世界

答え合わせ

- $\mathbb{F}_7$ の掛け算の演算表を完成させよ. ($\bullet$ を省略しています.)

$\times$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{4}$	$\mathbf{5}$	$\mathbf{6}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{4}$	$\mathbf{5}$	$\mathbf{6}$
$\mathbf{2}$	$\mathbf{0}$	$\mathbf{2}$	$\mathbf{4}$	$\mathbf{6}$	$\mathbf{1}$	$\mathbf{3}$	$\mathbf{5}$
$\mathbf{3}$	$\mathbf{0}$	$\mathbf{3}$	$\mathbf{6}$	$\mathbf{2}$	$\mathbf{5}$	$\mathbf{1}$	$\mathbf{4}$
$\mathbf{4}$	$\mathbf{0}$	$\mathbf{4}$	$\mathbf{1}$	$\mathbf{5}$	$\mathbf{2}$	$\mathbf{6}$	$\mathbf{3}$
$\mathbf{5}$	$\mathbf{0}$	$\mathbf{5}$	$\mathbf{3}$	$\mathbf{1}$	$\mathbf{6}$	$\mathbf{4}$	$\mathbf{2}$
$\mathbf{6}$	$\mathbf{0}$	$\mathbf{6}$	$\mathbf{5}$	$\mathbf{4}$	$\mathbf{3}$	$\mathbf{2}$	$\mathbf{1}$

- $\mathbb{F}_7$ で $\overline{\mathbf{2}} \div \overline{\mathbf{3}}$ を計算しなさい.
  掛け算の表より, $\overline{\mathbf{3}}$ の逆数は $\mathbf{5}$ だから,

$$\overline{\mathbf{2}} \div \overline{\mathbf{3}} = \overline{\mathbf{2}} \times \overline{\mathbf{5}} = \overline{\mathbf{10}} = \overline{\mathbf{3}}.$$

答え合わせ

- $\mathbb{F}_7$ で方程式 $\overline{5}x + \overline{4} = -x + \overline{1}$ を解け.
  移項して, $\overline{5}x + x = \overline{1} - \overline{4}$.
  整理して, $\overline{6}x = \overline{-3} = \overline{4}$.
  したがって, $x = \overline{4} \div \overline{6} = \overline{4} \times \overline{6} = \overline{24} = \overline{3}$.
- $\mathbb{F}_7$ で方程式 $x^2 + x + \overline{1} = \overline{0}$ を解け.
  $\overline{1} = -\overline{6}$ なので, 方程式は

$$x^2 + x - \overline{6} = \overline{0}$$
$$(x - \overline{2})(x + \overline{3}) = \overline{0}$$

と変形でき, このとき, $x - \overline{2} = \overline{0}$ または $x + \overline{3} = \overline{0}$ となるので,

$$x = \overline{2}, \overline{4}.$$

余りの世界

発展的なお話

- いままで, 素数で割った余りの世界だけを考えてきたが, $n = 6$ などの合成数 (=素数でない数) で割った余りの世界も考えることができる. この余りの世界は $\mathbb{Z}/n\mathbb{Z}$ という記号で表される :

$$\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}.$$

- 先ほど, $\mathbb{F}_7$ で 2 次方程式を解くときに,

$$\overline{n} \times \overline{m} = \overline{0} \text{ なら } \overline{n} = \overline{0} \text{ または } \overline{m} = \overline{0}$$

という「当たり前」に思える性質を利用した. 実は, この性質は合成数で割った世界では正しくない. 例えば, $\mathbb{Z}/6\mathbb{Z}$ では

$$\overline{2} \times \overline{3} = \overline{6} = \overline{0}$$

のように, $\overline{0}$ でない 2 つの数を掛けて, $\overline{0}$ になってしまうことがある.

$\mathbb{F}_p$ における不定方程式 $x^2 + y^2 = 1$

$x^2 + y^2 = 1$ を $\mathbb{F}_p$ で考えよう

- 最後に, 余りの世界 $\mathbb{F}_p$ において, 不定方程式 $x^2 + y^2 = 1$ の解がいくつあるのかを調べてみよう.
- とくに, p を変えると, 解の個数がどう変わるかを調べてみよう.
- 第 1 部で有理数に対して考えたことを踏まえると, この問題は, $\mathbb{F}_p$ の世界で「座標平面」を考えたときに, 「円」$x^2 + y^2 = 1$ の上にいくつの「$\mathbb{F}_p$ 点」があるのか, という問題を考えることに対応する.

$\mathbb{F}_p$ における不定方程式 $x^2 + y^2 = 1$

$\mathbb{F}_5$ で $x^2 + y^2 = 1$ の解はいくつある？

- 第 2 部で考えた演算表の, 対角線の部分だけ取り出して, 平方数の表を作る.

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\Rightarrow$

n	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
n^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{4}$	$\overline{1}$

- 平方数 (下の行の数) であって, 2 つ足すと 1 になる組み合わせを探す.

n	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
n^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{4}$	$\overline{1}$

n	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
n^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{4}$	$\overline{1}$

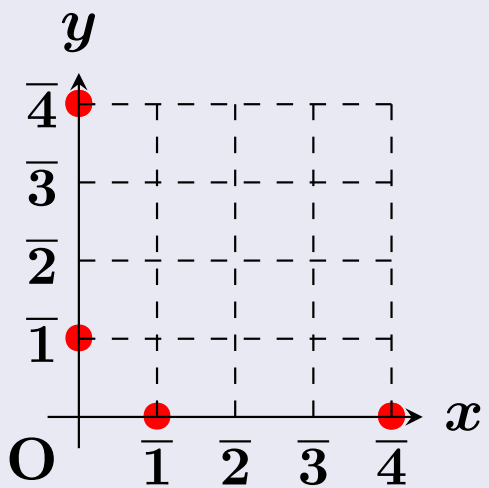
$\mathbb{F}_p$ における不定方程式 $x^2 + y^2 = 1$

$\mathbb{F}_5$ で $x^2 + y^2 = 1$ の解はいくつある？

- $\overline{0}^2 + \overline{1}^2 = \overline{1},\ \overline{1}^2 + \overline{0}^2 = \overline{1},\ \overline{0}^2 + \overline{4}^2 = \overline{1},\ \overline{4}^2 + \overline{0}^2 = \overline{1}$
  だから, $\mathbb{F}_5$ において, $x^2 + y^2 = 1$ の解は

$$(x, y) = (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{0}, \overline{4}), (\overline{4}, \overline{0})$$

  の 4 個あることが分かる.
- 「円」$x^2 + y^2 = 1$ 上の $\mathbb{F}_5$ 点を図示すると次のようになる：



$\mathbb{F}_p$ における不定方程式 $x^2 + y^2 = 1$

Example ($\mathbb{F}_{13}$ で $x^2 + y^2 = 1$ の解はいくつある？)

n	0	1	2	3	4	5	6	7	8	9	10	11	12
n^2	0	1	4	9	3	12	10	10	12	3	9	4	1

- 下の行に出てきた数字で, 足して 1 になる組み合わせは,

$$\overline{0} + \overline{1} = \overline{4} + \overline{10} = \overline{1}.$$

- したがって, $x^2 + y^2 = 1$ を満たす組み合わせは,

$$(x, y) = (0, 1), (0, 12), (2, 6), (2, 7), (11, 6), (11, 7)$$

と, この座標の x と y を入れ替えたものなので, $6 \times 2 =$12 個となる.

$\mathbb{F}_p$ における不定方程式 $x^2 + y^2 = 1$

Example ($\mathbb{F}_{19}$ で $x^2 + y^2 = 1$ の解はいくつある？)

n	0	1	2	3	4	5	6	7	8	9
n^2	0	1	4	9	16	6	17	11	7	5

n	10	11	12	13	14	15	16	17	18
n^2	5	7	11	17	6	16	9	4	1

- 下の行に出てきた数字で, 足して 1 になる組み合わせは,

$$\overline{0} + \overline{1} = \overline{4} + \overline{16} = \overline{9} + \overline{11} = \overline{1}.$$

- したがって, $x^2 + y^2 = 1$ を満たす組み合わせは,

$$\begin{aligned}(x, y) =& (0, 1), (0, 18), (2, 4), (2, 15), (17, 4),\\ & (17, 15), (3, 7), (3, 12), (16, 7), (16, 12)\end{aligned}$$

と, この座標の x と y を入れ替えたものなので, $10 \times 2 =$20 個となる.

$\mathbb{F}_p$ における不定方程式 $x^2 + y^2 = 1$

各 $\mathbb{F}_p$ での $x^2 + y^2 = 1$ の解の個数

p	**3**	**5**	**7**	**11**	**13**	**17**	**19**
解の個数	?	**4**	?	?	**12**	?	**20**
p との差	?	-1	?	?	-1	?	$+1$

Quiz 5

$p = 3, 7, 11, 17$ の場合に, $x^2 + y^2 = 1$ の解の個数はいくつだろうか？
また, 解の個数は p と比較してどうなっているか？

$\mathbb{F}_p$ における不定方程式 $x^2 + y^2 = 1$

各 $\mathbb{F}_p$ での n^2 の数表

- $p = 3$ のとき

n	0	1	2
n^2	0	1	1

- $p = 7$ のとき

n	0	1	2	3	4	5	6
n^2	0	1	4	2	2	4	1

- $p = 11$ のとき

n	0	1	2	3	4	5	6	7	8	9	10
n^2	0	1	4	9	5	3	3	5	9	4	1

- $p = 17$ のとき

n	0	1, 16	2, 15	3, 14	4, 13	5, 12	6, 11	7, 10	8, 9
n^2	0	1	4	9	16	8	2	15	13

$\mathbb{F}_p$ における不定方程式 $x^2 + y^2 = 1$

答え合わせ

p	3	5	7	11	13	17	19
解の個数	4	4	8	12	12	16	20
p との差	$+1$	-1	$+1$	$+1$	-1	-1	$+1$

- ここまでを見る限り, $x^2 + y^2 = 1$ の解の個数は p がいくつであっても, $p+1$ または $p-1$ になっている.
- いつ $p+1$ になり, いつ $p-1$ になるのだろう？ 実は...

p を 4 で割った余りを見てみると...！

p	3	5	7	11	13	17	19
解の個数	4	4	8	12	12	16	20
p との差	$+1$	-1	$+1$	$+1$	-1	-1	$+1$
p を 4 で割った余り	3	1	3	3	1	1	3

$\mathbb{F}_p$ における不定方程式 $x^2 + y^2 = 1$

まとめ ($\mathbb{F}_p$ での $x^2 + y^2 = 1$ の解の個数)

p を素数とする. $\mathbb{F}_p$ における不定方程式 $x^2 + y^2 = 1$ の解の個数には次の法則がある：

$$\begin{cases} p \text{ 個} & p = 2 \text{ のとき} \\ p - 1 \text{ 個} & p \text{ を } 4 \text{ で割った余りが } 1 \text{ のとき} \\ p + 1 \text{ 個} & p \text{ を } 4 \text{ で割った余りが } 3 \text{ のとき} \end{cases}$$

Example

素数 101 を考える. 101 を 4 で割った余りは 1 だから, この規則性によれば, 数え上げることなく (!), $\mathbb{F}_{101}$ における $x^2 + y^2 = 1$ の解の個数は

$$101-1 = 100\text{個}$$

と求めることができる.

$\mathbb{F}_p$ における不定方程式 $x^2 + y^2 = 1$

発展的なお話

このきれいな法則は

- 第 1 部で, ピタゴラス数の公式を作るときに出てきた交点の話が余りの世界でも全く同じように成り立つこと：

  「円」 $x^2 + y^2 = 1$ 上の $(-1, 0)$ 以外の $\mathbb{F}_p$ 点は,

  $\mathbb{F}_p$ の数 t から $\left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right)$ によってすべて作られる

- $\mathbb{F}_p$ には 2 乗すると -1 になる数がない
  $\Leftrightarrow$ p を 4 で割った余りが 3 である.

という 2 つの事実から導かれる. 2 つ目の事実は, 今回の講演では紹介できなかったが, 「平方剰余の相互法則と補充則」と呼ばれる, 余りの世界における平方数を決定する不思議な規則性がその背景にある.

参考文献

- 今回のテーマに関連する読み物：
  - 芹沢正三, 『素数入門-計算しながら理解できる』, 講談社 (ブルーバックス), 2002.
  - 足立恒雄, 『フェルマーの大定理が解けた!-オイラーからワイルズの証明まで』, 講談社 (ブルーバックス), 1995.
  - 吉永良正, 『数学・まだこんなことがわからない-素数の謎から森理論まで』, 講談社 (ブルーバックス), 1990.
    ※ 新装版が出ているようです.
- 今回のテーマについてより深く学習するためのテキスト：
  - 山崎隆雄, 『初等整数論 数論幾何への誘い』, 共立講座 (数学探検 6), 共立出版, 2015.
  - 雪江明彦, 『整数論 1: 初等整数論から p 進数へ』, 日本評論社, 2013.
  - 高木貞治, 『初等整数論講義』(第 2 版), 共立出版, 1971.

ありがとうございました