整数論
素数の密度と素数の判定法

2005MM064 柴田直哉
指導教員：宮元忠敏

1　はじめに

素数には生成規則がないため, 1 変数の数式に自然数を順に代入して素数を順に出力することは不可能だということはわかっている. また, 素数は無限に存在することも本研究では学ぶ. しかしながら, まだ見つかっていない素数もいまだにあることも事実である. このような不思議な素数という数をエラトステネスのふるい法よりも簡単な方法で見つけだすことができればおもしろいだろうと考えた. そこで本研究では, 素数判定の方法を理解し, それを $Mathematica$ のプログラムを利用し検証することで, より正確でより計算量が少なくてすむ素数判定テストを考えることを目的としている.

2　素数

素数とは, 2 以上の整数で 1 と自分以外の約数をもたないものであり, 以下のようなものがある.

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, \cdots$

2.1　素数の密度

予想

自然数 m の付近には $\frac{1}{\log m}$ の割合で素数が存在することが予想できる.

2.2　素数の無限性

定理 (オイラー)

$$\sum_{p:\text{素数}} \frac{1}{p} \text{ は発散する.}$$

とくに素数は無限に存在する.

3　群論

群　… ある規則によって $a, b \in G$ に対して G の元が一つ定められている. このとき a, b に対して定まる元を $a \circ b$ と表す.

群の位数 … 群 G を構成している元の個数.

部分群…群 G の部分集合 H で同じ演算で群になるもの.

剰余類　aH … G の部分群 H に対し, G のある元 a によって $\{a \circ h \mid h \in H\}$ と表される集合.

元の位数 … 群 G の元 a に対して $a, a^2, a^3, a^4, \cdots$ と作っていって初めて単位元になったときの掛けた a の個数.

巡回群 … $a, a^2, a^3, a^4, \cdots, a^n = e$ の n 個の元からなる集合は a を生成元とする巡回群という.

既約剰余類　$(Z/mZ)^*$ … Z の mZ による剰余類 $a+mZ$ で $GCD(a, m) = 1$ となるもの.

定理

H が群 G の部分群であるならば, H の位数は G の位数の約数である.

G の位数 $= H$ の位数　×　異なる剰余類群の個数

定理

元の位数は群の位数の約数である.

4　フェルマーテスト

フェルマーの小定理

素数 p に対して $GCD(a, p) = 1$ ならば

$$a^{p-1} \equiv 1 \quad mod\ p$$

である.

$$\begin{aligned} n \text{ が素数である} &\Longrightarrow \forall a\ (1 \leq a \leq n-1) \\ &\quad a^{n-1} \equiv 1 \quad mod\ n \\ &\Longrightarrow \exists a\ (1 \leq a \leq n-1) \\ &\quad a^{n-1} \equiv 1 \quad mod\ n \end{aligned}$$

逆を考えると

$$a^{n-1} \equiv 1 \quad mod\ n$$

となる n は素数になるとは限らない. ただし, 素数である可能性は高い.

フェルマーテスト

自然数 n がある自然数 a に対して

$$a^{n-1} \equiv 1 \quad mod\ n$$

になったら n は a を底とするフェルマーテストを通ったという.

カーマイケル数… 合成数でありながら, $GCD(a, n) = 1$ となるすべての a を底として, フェルマーテストを通る数をいう.

5　平方剰余記号

素数 p に対し p の倍数でない整数 a が $mod\ p$ の**平方剰余**であるとは

$$s^2 \equiv a \quad mod\ p$$

となる整数 s が存在することである.

このような s が存在しないとき a は $mod\ p$ の**平方非剰余**であうという.

a が p の倍数であるときは平方剰余であるとも平方非剰余であるともいわない.

次のように定めた関数を**平方剰余記号**あるいは**ルジャンドル記号**という.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ が } mod\ p \text{ の平方剰余のとき} \\ -1 & a \text{ が } mod\ p \text{ の平方非剰余のとき} \\ 0 & a \text{ が } mod\ p \text{ の倍数のとき} \end{cases}$$

a は任意の整数で,p は素数とする.

定理　オイラーの規準

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \quad mod\ p$$

6　ヤコビ記号

奇数 m が $m = \prod_{i=1}^{r} p_i$ という形の素数の積であるとき, (このとき, 素数は同じものであってもよい)

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)$$

と定義して, 平方剰余記号を奇数の合成数にまで拡張する. これを**ヤコビ記号**という.
とくに m が素数 p のとき

$$\text{ヤコビ記号} \left(\frac{a}{p}\right) = \text{平方剰余記号} \left(\frac{a}{p}\right)$$

平方剰余記号で成り立つ法則はヤコビ記号でも成り立つ.

7　オイラーテスト

オイラーの規準より

$$\begin{aligned} n \text{ が素数である} &\Longrightarrow \forall a\ (1 \le a \le n-1) \\ &\quad a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \quad mod\ n \\ &\Longrightarrow \exists a\ (1 \le a \le n-1) \\ &\quad a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \quad mod\ n \end{aligned}$$

逆を考えると,

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \quad mod\ n$$

となる n は必ずしも素数になるとは限らない. ただし, 素数である可能性は高い.

オイラーテスト

奇数 n がある整数 a に対して

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \quad mod\ n$$

となったら a は n を底とするオイラーテストを通ったという.

8　素数判定

Mathematica プログラムを用いてフェルマーテストとオイラーテストの精度を比較する.
1 から 1000000 の数までの数に対して 2,3,5,7 を底とするフェルマーテストとオイラーテストを行った際に合成数でありながら, テストを通るものを誤答として, その数を比較する.

底	フェルマーテストでの誤答数	オイラーテストでの誤答数
2	78	36
2&3	23	9
2&3&5	11	3
2&3&5&7	4	0

オイラーテストはヤコビ記号を使う分フェルマーテストより計算量が多いが, 誤答数が少ないことから信頼度が高いことがわかる.

定理

奇数 n が $GCD(a,n) = 1$ となるすべての a に対して
$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \quad mod\ n$
となったなら n は素数である.

したがって, オイラーテストには合成数でありながら $GCD(a,n) = 1$ となるすべての a を底としてテストを通る数はない.

9　おわりに

本研究では, オイラーテストにはフェルマーテストのカーマイケル数のように合成数でありながら, 互いに素な底をすべて通る数は存在しないことがわかった. なのですべての底においてオイラーテストを実施すれば必ず素数か合成数かを判断できることがわかった. しかしながら, オイラーテストはヤコビ記号を利用しているため, かなりの計算量が必要だということもいえる. そのため, 大きな素数を発見することは困難である.
本研究を通して, 素数の奥深さやおもしろさがわかった. 今後の課題としてさらに計算量が少なく, 効率のよい素数判定法を探していきたい.

参考文献

[1] 木田祐司 :『講座—数学の考え方１６　初等整数論』. 朝倉書店, 東京, 2001.

[2] 山本芳彦 :『現代数学への入門　数論入門』. 岩波書店, 東京, 2003.

[3] 斎藤正彦 :『はじめての群論』. 日本評論社, 東京, 2005.

[4] 吉田賢史 :『かんたん *Mathematica* 活用ガイド』. 東京電気大学出版局, 東京, 2000.

[5] 山田修司 :『*Mathematica* で楽しむ数理科学』. 牧野書店, 東京, 1999.