素数生成多項式

大手前高校

背景

きっかけ

オイラーの数式

$$f(n) = n^2 - n + 41$$

スゴイ!!

f(n)が0≦n<41で素数になる

f(n) = n^2 − n + pの形では
この式が0から連続して一番多く素数を生み出す
ことが知られている。これは虚二次体Q(√-163)
の類数が1であることと関係している

研究テーマ

ルビーの数式

$$f(n) = 36n^2 - 810n + 2753$$

f(n)が0≦n<45で絶対値が素数になる

f(n) = an^2 + bn + cの形では
この式が最高記録かはわかっていない

もしかしたら、記録超えられるかも？？

GOAL

Rubyの記録を**超えて**
46個以上連続して素数を
生み出す式を作る

$$f(n) = an^2 + bn + c$$

$f(0)$ = 素数
$f(1)$ = 素数
$f(2)$ = 素数
⋮
$f(43)$ = 素数
$f(44)$ = 素数
$f(45)$ = 素数

アイデア

$$f(n) = an^2 + bn + c$$

① Cは素数

n=0のとき　f(0)=c　になるためcは素数である必要がある

② 合同式使ってみた

２次合同方程式の可解性

aはpで割り切れない数とする

an^2+bn+c≡0 (mod p)は
D=b^2-4acがpを法として
平方剰余のとき、解をもち
平方非剰余のとき解をもたない

ということは…

b^2-4acがいろんな素数の平方非剰余だったら
f(n)は割り切れにくくなる

特に45以下の素数の平方非剰余が望ましい

簡単な説明

この合同式が解をもつとは
an^2+bn+cがpの倍数となる非負整数nがp以下に
存在するということ

↓

今回の場合では少なくともn≦45に解が存在すると
記録を越えられないのでDが45以下の素数の
平方剰余となると少し困る

少し困る？

実はaがpで割り切れないときに限っているので
「a,bを5の倍数にするなどの条件を加えると
Dが5を法とした平方剰余でも大丈夫」
といった条件の選別ができる！

③ a,bは2の倍数

2の平方非剰余はないのでa,bは2の倍数
でなければならない

採用した条件

・cは素数
・a,bは2の倍数
・a,bは3の倍数
・b^2-4acは5〜43まで全ての素数の平方非剰余

これらの条件を採用することでnが45以下のときf(n)は43以下の素数では割り切れない

また、a,bを3の倍数とすることで3を法とする平方非剰余の条件を回避したこれによって条件を満たすDがふえると考えた

同じことを5以上の素数で行わなかった理由は単純にn^2の係数が大きくなってしまいf(n)の値が大きくなりすぎることを防ぐため

実際にルビーの式も　D=b^2-4acは　5〜43 の平方非剰余となっていた

実験

一部計算にコンピューター使用

アイデアで求めた必要条件を満たすDを求めると…

D=　36132
144528
259668
325188
⋮

一つ選んで

$$b^2 - 4ac = D$$

となるように適当なa,b,cの組み合わせを求める

(a,b,cの条件もふまえる)

$$f(n) = an^2 + bn + c$$

式が完成したら代入して記録を確認する

Ruby

D	36132	259668	144528	259668	358728	325188	491532
A	24	36	12	36	6	72	6
B	210	-810	-528	510	600	582	702
C	83	2753	2797	3	53	47	53

今回見つけた数式たち

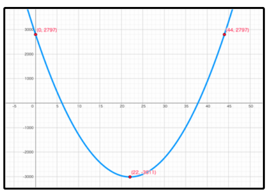
f(n)=24n^2+210n+83
f(n)=36n^2-810n+2753
f(n)=12n^2-528n+2797
f(n)=36n^2+510n+3
f(n)=6n^2+600n+53
f(n)=72n^2+582n+47
f(n)=6n^2+702n+53

結論

$$f(n) = 12n^2 - 528n + 2797$$

$f(0) = 2797$	$f(10) = -1283$	$f(20) = -2963$	$f(30) = -2243$	$f(40) = 877$
$f(1) = 2281$	$f(11) = -1559$	$f(21) = -2999$	$f(31) = -2039$	$f(41) = 1321$
$f(2) = 1789$	$f(12) = -1811$	$f(22) = -3011$	$f(32) = -1811$	$f(42) = 1789$
$f(3) = 1321$	$f(13) = -2039$	$f(23) = -2999$	$f(33) = -1559$	$f(43) = 2281$
$f(4) = 877$	$f(14) = -2243$	$f(24) = -2963$	$f(34) = -1283$	$f(44) = 2797$
$f(5) = 457$	$f(15) = -2423$	$f(25) = -2903$	$f(35) = -983$	$f(45) = 3337$
$f(6) = 61$	$f(16) = -2579$	$f(26) = -2819$	$f(36) = -659$	
$f(7) = -311$	$f(17) = -2711$	$f(27) = -2711$	$f(37) = -311$	
$f(8) = -659$	$f(18) = -2819$	$f(28) = -2579$	$f(38) = 61$	
$f(9) = -983$	$f(19) = -2903$	$f(29) = -2423$	$f(39) = 457$	

n=45は47で割れるため
素数ではない



0≦ n ≦44で45個連続して素数を生み出す
Rubyさんに並ぶ世界1位タイの記録

今後の展望

本研究では、Rubyと同様に45個連続して素数を生成する式を構築することができた。また研究過程よりRubyの記録を超えるためにはより厳密な条件を設定し、それに基づいて多項式を改良する必要がある。

① なぜ素数46個以上出す式を生成するのが難しいのか

→条件の設定が甘かった。ただし、条件が厳しくなると係数が大きくなって多項式の値が大きくなりすぎる可能性があるため
新たな記録を達成するのは容易ではない。

② 合同式を使わない方法で考える

今回はan^2+bn+c≡0 (mod p)が解を持たないとき、判別式(D)=b^2-4acがpの平方非剰余であることを利用した。今後は合同式以外の方法も用いて多角的な視点で考えていきたいと思う。

参考文献

平方剰余の相互法則と 2次(または3次)合同方程式の解について - 青山学院大学 理工学部 物理・数理学科 小野 駿輝 2023/2/20
https://www.math.aoyama.ac.jp/~kyo/sotsuken/2022/sotsuron_2022_OnoShunki.pdf
Paulo Ribenboim, 我が数、我が友よ：数論への招待, 共立出版, 2003.8