

7.11 たかが素因数分解，されど素因数分解

7.11.9 現状の素因数分解

7.11.9.2 2026 年後期編 (9 月末)

前回 2026 年 3 月から半年経ったのでどれくらい進歩があったのか `factor.db` で調べてみた。最初はカニンガムプロジェクト ($b^n \pm 1, b = 2, 3, 5, 6, 7, 10, 11, 12$) の数から紹介しよう。

- ① $2^{1207} - 1 = P_6 \times P_6 \times P_8 \times P_9 \times C_{337} \rightarrow C_{337} = P_{91} \times P_{247}$
- ② $3^{709} - 1 = 2^2 \times P_{12} \times C_{327} \rightarrow C_{327} = P_{159} \times P_{178}$
- ③ $6^{436} + 1 = 1297 \times P_9 \times P_{24} \times C_{258} \rightarrow C_{258} = P_{102} \times P_{157}$
- ④ $7^{397} + 1 = 2^3 \times P_{10} \times P_{13} \times P_{14} \times C_{300} \rightarrow C_{300} = P_{92} \times P_{208}$
- ⑤ $7^{398} + 1 = 2 \times 5^2 \times 797 \times C_{332} \rightarrow C_{332} = P_{137} \times P_{195}$
- ⑥ $7^{401} + 1 = 23 \times P_{13} \times P_{26} \times P_{41} \times C_{260} \rightarrow C_{260} = P_{81} \times P_{179}$
- ⑦ $11^{331} - 1 = 2 \times 5 \times C_{344} \rightarrow C_{344} = P_{136} \times P_{209}$
- ⑧ $12^{311} - 1 = 11 \times C_{335} \rightarrow C_{335} = P_{155} \times P_{181}$
- ⑨ $12^{313} - 1 = 11 \times P_6 \times P_7 \times P_{11} \times P_{32} \times C_{283} \rightarrow C_{283} = P_{75} \times P_{99} \times P_{109}$
- ⑩ $12^{319} - 1 = 11^2 \times 23 \times 59 \times 24767 \times P_6 \times P_9 \times P_9 \times P_{19} \times P_{35} \times C_{260} \rightarrow C_{260} = P_{75} \times P_{185}$

完全素因数分解は以上の 10 個の数が更新されていた。長年の懸案だった $2^{1207} - 1$ が素因数分解されていたのは驚きました。私がカニンガムプロジェクトとは別に公開してある数の素因数分解の状態も調べてみました。

- ⑤ $13^{241} - 1 = 2^2 \times 3 \times 1447 \times P_{23} \times C_{242} \rightarrow C_{242} = P_{74} \times P_{168}$
- ⑥ $15^{239} - 1 = 2 \times 7 \times 479 \times P_7 \times P_7 \times P_{19} \times C_{247} \rightarrow C_{247} = P_{49} \times P_{198}$

これ以外にも公開はしていないが素因数分解できない数として記録してあった $13^{305} - 1$ と $13^{277} + 1$ が素因数分解できるようになっていた。

式	整数列大辞典	前回範囲	現在範囲	次の合成数	式	整数列大辞典	前回範囲	現在範囲	次の合成数
$2^n - 1$	A005420	1206	1212	C_{297}	$2^n + 1$	A002587	1128		C_{330}
$3^n - 1$	A074477	730		C_{265}	$3^n + 1$	A074476	708	711	C_{330}
$5^n - 1$	A074479	502		C_{260}	$5^n + 1$	A074478	487		C_{301}
$6^n - 1$	A274907	436		C_{273}	$6^n + 1$	A274904	435	438	C_{270}
$7^n - 1$	A074249	420		C_{305}	$7^n + 1$	A227575	396	411	C_{316}
$10^n - 1$	A005422	352		C_{328}	$10^n + 1$	A003021	345		C_{300}
$11^n - 1$	A274910	330	340	C_{289}	$11^n + 1$	A062308	325		C_{334}
$12^n - 1$	A366718	310	330	C_{290}	$12^n + 1$	A366720	325		C_{347}

空欄は範囲に変化がないことを表しています。整数列大辞典の範囲も前回から更新されました。最後に私が独自に調べ公開している数についても前回 (2026 年 3 月) との違いを載せておきます。

式	整数列大辞典	前回範囲	現在範囲	次の合成数	式	整数列大辞典	前回範囲	現在範囲	次の合成数
$13^n - 1$		240	262	C_{278}	$13^n + 1$		228		C_{249}
$14^n - 1$		222		C_{247}	$14^n + 1$		222		C_{228}
$15^n - 1$		226		C_{254}	$15^n + 1$		217		C_{207}
$17^n - 1$		232		C_{245}	$17^n + 1$		211		C_{239}
$18^n - 1$		222		C_{279}	$18^n + 1$		210		C_{228}
$19^n - 1$		222		C_{259}	$19^n + 1$		201		C_{252}

7.11.9.2.1 RSA Factoring Challenge

以前に紹介した RSA の因数分解だが 2 つの数が因数分解されていた。日付は RSA-260 が 9 月 3 日で RSA-896 が 9 月 19 日でした。(英語版の Wikipedia より)

$$\text{RSA-260 } C_{260} = P_{130} \times P_{130}$$

```
2211282552952966643528108525502623092761208950247001539441374831912882294140200198651272972656974659
9085900330031400051170742204560859276357953757185954298838958709229238491006703034124620545784566413
664540684214361293017694020846391065875914794251435144458199
= 4397328654844826923795068102505872571721883526553349659561256924505973939597593482272505698004801207
988043088656411102133523080581
× 5028695206842569864686141618253083416610081090075366674776775706538324961364412200138116378509733307
971876652984898985905923678379
```

$$\text{RSA-896 } C_{270} = P_{135} \times P_{135}$$

```
412023436986659543855531365332575948179811699844327982845455626433876445565248426198098870423161841
879261420247188869492560931776375033421130982397485150944909106910269861031862704114880866970564902
903653658867433731720813104105190864254793282601391257624033946373269391
= 636606729769440499166579950236036751749912014371509557713570027508971809534551913252252094954941974
952859310861988904737359709200557919
× 647218161102195448058768698177623951380616936266986989243011933572862870905830904361851542450154852
431416136790787107595965374752513489
```