30n+P 形式のエラトステネスの篩

八野 正

2009 年 12 月 30 日

第1章　素数候補

以下の説明において全ての変数は自然数である。

1.1　素数候補式 30n+P

素数は、$6n \pm 1$ が、2 と 3 の倍数を除いた一般形式の素数候補式である。
同様に、$30n + P$ が、2 と 3 と 5 の倍数を除いた一般形式の素数候補式である。

ここで、P は、30 未満の 2,3,5 で割り切れない数である。
すなわち、

1. $P = 2a + 1$
2. $P = 3b + 1$,$P = 3b + 2$ のいずれかを満足するもの
3. $P = 5c + 1$,$P = 5c + 2$,$P = 5c + 3$,$P = 5c + 4$ のいずれかを満足するもの

以上 1,2,3 の全ての条件を満足するものである。
したがって、$1 \times 2 \times 4 = 8$ の組合せがある。

以下に P の値の表を示す。

2a+1	5c+1	5c+2	5c+3	5c+4
3b+1	1	7	13	19
3b+2	11	17	23	29

元に戻って $30n + P$ を考えると、$30n + P = 2 \times (15n + \frac{P}{2})$ において P は 2 で割り切れないので $30n + P$ は 2 でわりきれない。
同様に、$30n + P = 3 \times (10n + \frac{P}{3})$ において P は 3 で割り切れないので $30n + P$ は 3 でわりきれない。
また、$30n + P = 5 \times (6n + \frac{P}{5})$ において P は 5 で割り切れないので $30n + P$ は 5 でわりきれない。
よって、$30n + P$ が、2 と 3 と 5 の倍数を除いた一般形式の素数候補式になる。

1.2　素数でないもの

さて、素数でないものは、素数同士の積に因数分解される。したがって、

$$(30a + l) = (30b + m)(30c + n) \tag{1.1}$$

が成り立つ必要がある。以下に検討結果を示す。

1. $(30m+1)(30k+1) = (900mk+30m+30k)+1$
   $= 30(30mk+m+k)+1 = 30p+1$ ただし、$p = 30mk+m+k$

2. $(30m+1)(30k+7) = (900mk+30k+7\times 30m)+7$
   $= 30(30mk+k+7m)+7 = 30p+7$ ただし、$p = 30mk+k+7m$

3. $(30m+1)(30k+11)$
   $= 30(30mk+k+11m)+11 = 30p+11$ ただし、$p = 30mk+k+11m$ 以下省略

4. $(30m+1)(30k+13) = 30p+13$

5. $(30m+1)(30k+17) = 30p+17$

6. $(30m+1)(30k+19) = 30p+19$

7. $(30m+1)(30k+23) = 30p+23$

8. $(30m+1)(30k+29) = 30p+29$

9. $(30m+7)(30k+1) = 30p+7$

10. $(30m+7)(30k+7) = 30p+49 = 30(p+1)+19$

11. $(30m+7)(30k+11) = 30p+77 = 30(p+2)+17$

12. $(30m+7)(30k+13) = 30p+91 = 30(p+3)+1$

13. $(30m+7)(30k+17) = 30p+119 = 30(p+3)+29$

14. $(30m+7)(30k+19) = 30p+133 = 30(p+4)+13$

15. $(30m+7)(30k+23) = 30p+161 = 30(p+5)+11$

16. $(30m+7)(30k+29) = 30p+203 = 30(p+6)+23$

17. $(30m+11)(30k+1) = 30p+11$

18. $(30m+11)(30k+7) = 30p+77 = 30(p+2)+17$

19. $(30m+11)(30k+11) = 30p+121 = 30(p+4)+1$

20. $(30m+11)(30k+13) = 30p+143 = 30(p+4)+23$

21. $(30m+11)(30k+17) = 30p+187 = 30(p+6)+7$

22. $(30m+11)(30k+19) = 30p+209 = 30(p+6)+29$

23. $(30m+11)(30k+23) = 30p+253 = 30(p+8)+11$

24. $(30m+11)(30k+29) = 30p+319 = 30(p+10)+19$

25. $(30m+13)(30k+1) = 30p+13$

26. $(30m+13)(30k+7) = 30p+91 = 30(p+3)+1$

27. $(30m+13)(30k+11) = 30p+143 = 30(p+4)+23$

28. $(30m+13)(30k+13) = 30p+169 = 30(p+5)+19$

29. $(30m+13)(30k+17) = 30p+221 = 30(p+7)+11$

30. $(30m+13)(30k+19) = 30p+247 = 30(p+8)+7$

31. $(30m+13)(30k+23) = 30p+299 = 30(p+9)+29$

32. $(30m+13)(30k+29) = 30p+377 = 30(p+12)+17$

33. $(30m+17)(30k+1) = 30p+17$

34. $(30m+17)(30k+7) = 30p+119 = 30(p+6)+29$

35. $(30m+17)(30k+11) = 30p+187 = 30(p+6)+7$

36. $(30m+17)(30k+13) = 30p+221 = 30(p+7)+11$

37. $(30m+17)(30k+17) = 30p+289 = 30(p+9)+19$

38. $(30m+17)(30k+19) = 30p+323 = 30(p+10)+23$

39. $(30m+17)(30k+23) = 30p+391 = 30(p+13)+1$

40. $(30m+17)(30k+29) = 30p+493 = 30(p+16)+13$

41. $(30m+19)(30k+1) = 30p+19$

42. $(30m+19)(30k+7) = 30p+133 = 30(p+4)+13$

43. $(30m+19)(30k+11) = 30p+209 = 30(p+6)+29$

44. $(30m+19)(30k+13) = 30p+247 = 30(p+8)+7$

45. $(30m+19)(30k+17) = 30p+323 = 30(p+10)+23$

46. $(30m+19)(30k+19) = 30p+361 = 30(p+12)+1$

47. $(30m+19)(30k+23) = 30p+437 = 30(p+14)+17$

48. $(30m+19)(30k+29) = 30p+551 = 30(p+18)+11$

49. $(30m+23)(30k+1) = 30p+23$

50. $(30m+23)(30k+7) = 30p+161 = 30(p+5)+11$

51. $(30m+23)(30k+11) = 30p+253 = 30(p+8)+13$

52. $(30m+23)(30k+13) = 30p+299 = 30(p+9)+29$

53. $(30m+23)(30k+17) = 30p+391 = 30(p+13)+1$

54. $(30m+23)(30k+19) = 30p+437 = 30(p+14)+17$

55. $(30m+23)(30k+23) = 30p+529 = 30(p+17)+19$

56. $(30m+23)(30k+29) = 30p+667 = 30(p+22)+7$

57. $(30m+29)(30k+1) = 30p+29$

58. $(30m+29)(30k+7) = 30p+203 = 30(p+6)+23$

59. $(30m+29)(30k+11) = 30p+319 = 30(p+10)+19$

60. $(30m+29)(30k+13) = 30p+377 = 30(p+12)+17$

61. $(30m+29)(30k+17) = 30p+493 = 30(p+16)+13$

62. $(30m+29)(30k+19) = 30p+551 = 30(p+18)+11$

63. $(30m+29)(30k+23) = 30p+667 = 30(p+22)+7$

64. $(30m+29)(30k+29) = 30p+841 = 30(p+28)+1$

いずれの場合も式 (1.1) を満足している。また、3 つ以上の素数の積に分解されるとき、式 (1.1) を適用すると積 2 つが 1 つになるので、結果として式 (1.1) に集約される。

第2章　エラトステネスの篩

2.1　30n+P の表と素数の倍数

さて、下に示す $30n + P$ の表の中から 7 の倍数の字体を濃くした。

n	P=1	P=7	P=11	P=13	P=17	P=19	P=23	P=29
0	1	**7**	11	13	17	19	23	29
1	31	37	41	43	47	**49**	53	59
2	61	67	71	73	**77**	79	83	89
3	**91**	97	101	103	107	109	113	**119**
4	121	127	131	**133**	137	139	143	149
5	151	157	**161**	163	167	169	173	179
6	181	187	191	193	197	199	**203**	209
7	211	**217**	221	223	227	229	233	239
8	241	247	251	253	257	**259**	263	269
9	271	277	281	283	**287**	289	293	299
10	**301**	307	311	313	317	319	323	**329**
11	331	337	341	**343**	347	349	353	359
12	361	367	**371**	373	377	379	383	389
13	391	397	401	403	407	409	**413**	419
14	421	**427**	431	433	437	439	443	449
15	451	457	461	463	467	**469**	473	479
16	481	487	491	493	**497**	499	503	509
17	**511**	517	521	523	527	529	533	**539**
18	541	547	551	**553**	557	559	563	569
19	571	577	**581**	583	587	589	593	599
20	601	607	611	613	617	619	**623**	629
21	631	**637**	641	643	647	649	653	659
22	661	667	671	673	677	**679**	683	689
23	691	697	701	703	**707**	709	713	719
24	**721**	727	731	733	737	739	743	**749**
25	751	757	761	**763**	767	769	773	779
26	781	787	**791**	793	797	799	803	809
27	811	817	821	823	827	829	**833**	839
28	841	**847**	851	853	857	859	863	869
29	871	877	881	883	887	**889**	893	899

ごらんのとおり 7 の倍数は縦に 7 個置きに並ぶ。

2.2　縦並びの証明

これは以下のように説明できる。

素数 $30n+p$ の倍数は、縦に並ぶとき横は 30 なので $30\times(30n+p)=30\times30n+30p$ より縦に並ぶ。
今、その間の $\frac{j}{k}$ にあるとすると縦に並ぶとき横は 30 なので、$30(30n+p)\frac{j}{k}=30(30n\frac{j}{k})+30p\frac{j}{k}$ となる。
$\frac{j}{k}<1$ なので $p\frac{j}{k}<p$
よって、$30p\frac{j}{k}<30p$ となり、縦には並ばないことになる。
すると、その間の $\frac{j}{k}$ にあるとすることはできない。
したがって、素数 $30n+p$ の倍数は縦に $30n+p$ ごとに並ぶ。

2.3　素数探索アルゴリズムの概要

まず、$30n+P$ の表を作る。以下において $a \mod b=c$ は自然数 a,b,c において a を b で割ったあまりを c とする。
まず表の最初の数 7 を取り出し、7 に $30n+P$ の表のはじめの数すなわち 7 をかける。49 を得る。
$(7\times7) \mod 30=49 \mod 30=19$ より、49 のあとは 56(8 列 $\times$ 7) 個おきに表の全ての数を消す。
次に表から 11 を得る。
$(7\times11) \mod 30=77 \mod 30=17$ より、77 のあとは 56 個おきに表の全ての数を消す。
次に表から 13 を得る。
$(7\times13) \mod 30=91 \mod 30=1$ より、91 のあとは 56 個おきに表の全ての数を消す。
このように 8 つの列を全て処理すれば、7 の倍数は除かれる。

次に、表から 7 の次の 11 を得る。
$(11\times11) \mod 30=121 \mod 30=1$ より、121 のあとは 88(8 列 $\times$ 11) 個おきに表の全ての数を消す。
次に表から 13 を得る。
$(11\times13) \mod 30=143 \mod 30=23$ より、143 のあとは 88 個おきに表の全ての数を消す。
このように 8 つの列を全て処理すれば、11 の倍数は除かれる。

これを $30n+P$ の表の残っている数をはじめから全てやれば完了する。