Part II Computational Projects 2020

C3318H

Attach to front of report

Project number:

15.10

15.10

Question 1

A program to check whether a number is B-smooth can be found in 1. We run the following script to find the probability that a d-digit integer is B-smooth where B is the set of primes less than 50. The result is shown in table 1.

```
B = [2 3 5 7 11 13 17 19 23 29 31 37 41 43 47];

for d = 1:9
    s = 0 ;
    for i = 10^(d-1) : 10^d - 1
        s = s + prod_primes(B,i) ;
    end
    fprintf('%d %4.2f \n', s, s/(9*10^(d-1)))
end
```

d	#B-smooth integers	$\mathbb{P}(B\text{-smooth})$
1	9	100.00%
2	80	88.89%
3	439	48.78%
4	1934	21.49%
5	7176	7.97%
6	23237	0.26%
7	67812	0.07%
8	181709	0.02%

Table 1: Probability of being B-smooth for randomly chosen d digit integers

Question 2

We apply induction on n. It's true for $n = 0$ by taking $r = 0$, $s = 1$. Suppose it's true for n and $x = \dfrac{r+\sqrt{N}}{s}$ with r, s integers and $s|(r^2N)$, we shall prove for $n+1$.
Now we are given $a_n = \lfloor x_n \rfloor$ and

$$\begin{aligned} x_{n+1} &= \frac{1}{x_n - a_n} \\ &= \frac{1}{\frac{r+\sqrt{N}}{s} - a_n} \\ &= \frac{(sa_n - r) + \sqrt{N}}{(N - (sa_n - r)^2)/s} \end{aligned}$$

So take $r' = sa_n - r$, $s' = \frac{N - r'^2}{s} = \frac{N - r^2}{s} - sa_n^2 + 2ra_n$, which is an integer. And we have $s'|(r'^2 N)$ from the definition of s' , so induction is done.

A program to find the first k partial quotients of the continued fraction of $\sqrt{N}$ can be found in page 2. named `cont_frac.m`. Table 2 shows the partial quotients of $\sqrt{N}$ for $1 \le N \le 50$.

We see that $\max r \le \lfloor \sqrt{N} \rfloor$ and $\max s \le 2\lfloor \sqrt{N} \rfloor$ for $1 \le N \le 50$.

N	Partial quotients	max r	max s
1	1,Inf,	1	1
2	1,2,2,2,2,2,2,2,2,2,2,2,2,2,2,	1	1
3	1,1,2,1,2,1,2,1,2,1,2,1,2,1,2,	1	2
4	2,Inf,	2	1
5	2,4,4,4,4,4,4,4,4,4,4,4,4,4,4,	2	1
6	2,2,4,2,4,2,4,2,4,2,4,2,4,2,4,	2	2
7	2,1,1,1,4,1,1,1,4,1,1,1,4,1,1,	2	3
8	2,1,4,1,4,1,4,1,4,1,4,1,4,1,4,	2	4
9	3,Inf,	3	1
10	3,6,6,6,6,6,6,6,6,6,6,6,6,6,6,	3	1
11	3,3,6,3,6,3,6,3,6,3,6,3,6,3,6,	3	2
12	3,2,6,2,6,2,6,2,6,2,6,2,6,2,6,	3	3
13	3,1,1,1,1,6,1,1,1,1,6,1,1,1,1,	3	4
14	3,1,2,1,6,1,2,1,6,1,2,1,6,1,2,	3	5
15	3,1,6,1,6,1,6,1,6,1,6,1,6,1,6,	3	6
16	4,Inf,	4	1
17	4,8,8,8,8,8,8,8,8,8,8,8,8,8,8,	4	1
18	4,4,8,4,8,4,8,4,8,4,8,4,8,4,8,	4	2
19	4,2,1,3,1,2,8,2,1,3,1,2,8,2,1,	4	5
20	4,2,8,2,8,2,8,2,8,2,8,2,8,2,8,	4	4
21	4,1,1,2,1,1,8,1,1,2,1,1,8,1,1,	4	5
22	4,1,2,4,2,1,8,1,2,4,2,1,8,1,2,	4	6
23	4,1,3,1,8,1,3,1,8,1,3,1,8,1,3,	4	7
24	4,1,8,1,8,1,8,1,8,1,8,1,8,1,8,	4	8
25	5,Inf,	5	1
26	5,10,10,10,10,10,10,10,10,10,10,10,10,10,10,	5	1
27	5,5,10,5,10,5,10,5,10,5,10,5,10,5,10,	5	2
28	5,3,2,3,10,3,2,3,10,3,2,3,10,3,2,	5	4
29	5,2,1,1,2,10,2,1,1,2,10,2,1,1,2,	5	5
30	5,2,10,2,10,2,10,2,10,2,10,2,10,2,10,	5	5
31	5,1,1,3,5,3,1,1,10,1,1,3,5,3,1,	5	6
32	5,1,1,1,10,1,1,1,10,1,1,1,10,1,1,	5	7
33	5,1,2,1,10,1,2,1,10,1,2,1,10,1,2,	5	8
34	5,1,4,1,10,1,4,1,10,1,4,1,10,1,4,	5	9
35	5,1,10,1,10,1,10,1,10,1,10,1,10,1,10,	5	10
36	6,Inf,	6	1
37	6,12,12,12,12,12,12,12,12,12,12,12,12,12,12,	6	1
38	6,6,12,6,12,6,12,6,12,6,12,6,12,6,12,	6	2
39	6,4,12,4,12,4,12,4,12,4,12,4,12,4,12,	6	3
40	6,3,12,3,12,3,12,3,12,3,12,3,12,3,12,	6	4
41	6,2,2,12,2,2,12,2,2,12,2,2,12,2,2,	6	5
42	6,2,12,2,12,2,12,2,12,2,12,2,12,2,12,	6	6
43	6,1,1,3,1,5,1,3,1,1,12,1,1,3,1,	6	9
44	6,1,1,1,2,1,1,1,12,1,1,1,2,1,1,	6	8
45	6,1,2,2,2,1,12,1,2,2,2,1,12,1,2,	6	9
46	6,1,3,1,1,2,6,2,1,1,3,1,12,1,3,	6	10
47	6,1,5,1,12,1,5,1,12,1,5,1,12,1,5,	6	11
48	6,1,12,1,12,1,12,1,12,1,12,1,12,1,12,	6	12
49	7,Inf,	7	1
50	7,14,14,14,14,14,14,14,14,14,14,14,14,14,14,	7	1

Table 2: Partial quotients of $\sqrt{N}$ for $1 \leq N \leq 50$

Question 3

Values of $P_n^2 - NQ_n^2$ is shown in table 3 for $N = 2, 13, 503, 1000, 78343, 896633$ and n up to 15.

n \ N	2	13	503	1000	78343	896633
1	-1	-4	-19	-39	-502	-1717
2	1	3	13	24	57	176
3	-1	-3	-31	-31	-422	-1339
4	1	4	2	25	101	463
5	-1	-1	-31	-36	-318	-328
6	1	4	13	9	213	893
7	-1	-3	-19	-24	-311	-989
8	1	3	1	25	122	136
9	-1	-4	-19	-4	-419	-703
10	1	1	13	25	33	904
11	-1	-4	-31	-24	-99	-821
12	1	3	2	9	298	869
13	-1	-3	-32	-36	-243	-808
14	1	4	12	25	209	943
15	-1	-1	-32	-31	-72	-600

Table 3: Values of $P_n^2 - NQ_n^2$

We can see that 1 appeared in the columns of $N = 2, 13, 503$ and -1 in $N = 2, 13$, which gives us solution for Pell and Negative Pell equation respectively.

If $N \equiv 3 \pmod 4$, then $P_n^2 - NQ_n^2 \equiv P_n^2 + Q_n^2 \not\equiv -1 \pmod 4$. So $N \equiv 3 \pmod 4$ ensures that the negative Pell equation is insoluble.

A program to find out whether $x^2 - Ny^2 = \pm 1$ can be found in page 14 named `is_1.m`. We compute $x^2 - Ny^2 - \epsilon \mod p$ for $\epsilon = \pm 1$ and $p = 1009, 1013, 1019, 1021, 1031$. Since the product of all these primes is larger than 10^{15}, we get equality if $x^2 - Ny^2 - \epsilon \mod p = 0$ for fixed $\epsilon = 1$ or -1.

A program to find solution of Pell's equation can be found in page 15 named `pell_solution.m`. Table 4, 5 and 6 shows the solutions found for $1 \le N \le 50$, $51 \le N \le 100$ and $500 \le N \le 550$ respectively.

N	Pell's solutions (P_n, Q_n)
1	
2	(3,2),(17,12),(99,70),(577,408),(3363,2378),(19601,13860),(114243,80782)
3	(2,1),(7,4),(26,15),(97,56),(362,209),(1351,780),(5042,2911),(18817,10864),
4	
5	(9,4),(161,72),(2889,1292),(51841,23184),(930249,416020),(16692641,7465176),
6	(5,2),(49,20),(485,198),(4801,1960),(47525,19402),(470449,192060),(4656965,1901198)
7	(8,3),(127,48),(2024,765),(32257,12192),(514088,194307),(8193151,3096720)
8	(3,1),(17,6),(99,35),(577,204),(3363,1189),(19601,6930),(114243,40391)
9	
10	(19,6),(721,228),(27379,8658),(1039681,328776),(39480499,12484830)
11	(10,3),(199,60),(3970,1197),(79201,23880),(1580050,476403),(31521799,9504180)
12	(7,2),(97,28),(1351,390),(18817,5432),(262087,75658),(3650401,1053780)
13	(649,180),(842401,233640),(1093435849,303264540),(1419278889601,393637139280),
14	(15,4),(449,120),(13455,3596),(403201,107760),(12082575,3229204)
15	(4,1),(31,8),(244,63),(1921,496),(15124,3905),(119071,30744),(937444,242047)
16	
17	(33,8),(2177,528),(143649,34840),(9478657,2298912),(625447713,151693352)
18	(17,4),(577,136),(19601,4620),(665857,156944),(22619537,5331476)
19	(170,39),(57799,13260),(19651490,4508361),(6681448801,1532829480)
20	(9,2),(161,36),(2889,646),(51841,11592),(930249,208010),(16692641,3732588)
21	(55,12),(6049,1320),(665335,145188),(73180801,15969360),(8049222775,1756484412)
22	(197,42),(77617,16548),(30580901,6519870),(12048797377,2568812232)
23	(24,5),(1151,240),(55224,11515),(2649601,552480),(127125624,26507525)
24	(5,1),(49,10),(485,99),(4801,980),(47525,9701),(470449,96030),(4656965,950599)
25	
26	(51,10),(5201,1020),(530451,104030),(54100801,10610040),(5517751251,1082120050)
27	(26,5),(1351,260),(70226,13515),(3650401,702520),(189750626,36517525)
28	(127,24),(32257,6096),(8193151,1548360),(2081028097,393277344)
29	(9801,1820),(192119201,35675640),(3765920568201,699313893460),
30	(11,2),(241,44),(5291,966),(116161,21208),(2550251,465610)
31	(1520,273),(4620799,829920),(14047227440,2522956527)
32	(17,3),(577,102),(19601,3465),(665857,117708),(22619537,3998607)
33	(23,4),(1057,184),(48599,8460),(2234497,388976),(102738263,17884436)
34	(35,6),(2449,420),(171395,29394),(11995201,2057160)
35	(6,1),(71,12),(846,143),(10081,1704),(120126,20305),(1431431,241956)
36	
37	(73,12),(10657,1752),(1555849,255780),(227143297,37342128)
38	(37,6),(2737,444),(202501,32850),(14982337,2430456),(1108490437,179820894)
39	(25,4),(1249,200),(62425,9996),(3120001,499600),(155937625,24970004)
40	(19,3),(721,114),(27379,4329),(1039681,164388),(39480499,6242415)
41	(2049,320),(8396801,1311360),(34410088449,5373952960)
42	(13,2),(337,52),(8749,1350),(227137,35048),(5896813,909898),(153090001,23622300)
43	(3482,531),(24248647,3697884),(168867574226,25752063645),
44	(199,30),(79201,11940),(31521799,4752090),(12545596801,1891319880)
45	(161,24),(51841,7728),(16692641,2488392),(5374978561,801254496
46	(24335,3588),(1184384449,174627960),(57643991108495,8499142809612),
47	(48,7),(4607,672),(442224,64505),(42448897,6191808),(4074651888,594349063)
48	(7,1),(97,14),(1351,195),(18817,2716),(262087,37829),(3650401,526890)
49	
50	(99,14),(19601,2772),(3880899,548842),(768398401,108667944)

Table 4: Solution of Pell's equation for $1 \leq N \leq 50$

N	Pell's solutions (P_n, Q_n)
51	(50,7),(4999,700),(499850,69993),(49980001,6998600),(4997500250,699790007)
52	(649,90),(842401,116820),(1093435849,151632270),(1419278889601,196818569640),
53	(66249,9100),(8777860001,1205731800),
54	(485,66),(470449,64020),(456335045,62099334),(442644523201,60236289960)
55	(89,12),(15841,2136),(2819609,380196),(501874561,67672752
56	(15,2),(449,60),(13455,1798),(403201,53880),(12082575,1614602)
57	(151,20),(45601,6040),(13771351,1824060),(4158902401,550860080)
58	(19603,2574),(768555217,100916244),(30131975818099,3956522259690),
59	(530,69),(561799,73140),(595506410,77528331),(631236232801,82179957720)
60	(31,4),(1921,248),(119071,15372),(7380481,952816),(457470751,59059220)
62	(63,8),(7937,1008),(999999,127000),(125991937,16000992),(15873984063,2015997992)
63	(8,1),(127,16),(2024,255),(32257,4064),(514088,64769),(8193151,1032240)
64	
65	(129,16),(33281,4128),(8586369,1065008),(2215249921,274767936)
66	(65,8),(8449,1040),(1098305,135192),(142771201,17573920)
67	(48842,5967),(4771081927,582880428),(466058366908226,56938091722785),
68	(33,4),(2177,264),(143649,17420),(9478657,1149456),(625447713,75846676)
69	(7775,936),(120901249,14554800),(1880014414175,226327139064),
70	(251,30),(126001,15060),(63252251,7560090),(31752504001,3795150120)
71	(3480,413),(24220799,2874480),(168576757560,20006380387),
72	(17,2),(577,68),(19601,2310),(665857,78472),(22619537,2665738)
73	(2281249,267000),(10408194000001,1218186966000),
74	(3699,430),(27365201,3181140),(202447753299,23534073290),
75	(26,3),(1351,156),(70226,8109),(3650401,421512),(189750626,21910515)
76	(57799,6630),(6681448801,766414740),(772362118440199,88596011107890),
77	(351,40),(246401,28080),(172973151,19712120),(121426905601,13837880160),
78	(53,6),(5617,636),(595349,67410),(63101377,7144824),(6688150613,757283934),
79	(80,9),(12799,1440),(2047760,230391),(327628801,36861120)
80	(9,1),(161,18),(2889,323),(51841,5796),(930249,104005),(16692641,1866294
81	
82	(163,18),(53137,5868),(17322499,1912950),(5647081537,623615832)
83	(82,9),(13447,1476),(2205226,242055),(361643617,39695544)
84	(55,6),(6049,660),(665335,72594),(73180801,7984680),(8049222775,878242206)
85	(285769,30996),(163327842721,17715391848),
86	(10405,1122),(216528049,23348820),(4505948689285,485888943078),
87	(28,3),(1567,168),(87724,9405),(4910977,526512),(274926988,29475267
88	(197,21),(77617,8274),(30580901,3259935),(12048797377,1284406116)
89	(500001,53000),(500002000001,53000106000),
90	(19,2),(721,76),(27379,2886),(1039681,109592),(39480499,4161610),
91	(1574,165),(4954951,519420),(15598184174,1635133995)
92	(1151,120),(2649601,276240),(6099380351,635904360)
93	(12151,1260),(295293601,30620520),(7176225079351,744139875780),
94	(2143295,221064),(9187426914049,947610731760),
95	(39,4),(3041,312),(237159,24332),(18495361,1897584),(1442400999,147987220)
96	(49,5),(4801,490),(470449,48015),(46099201,4704980),(4517251249,461040025)
97	(62809633,6377352),
98	(99,10),(19601,1980),(3880899,392030),(768398401,77619960)
99	(10,1),(199,20),(3970,399),(79201,7960),(1580050,158801),(31521799,3168060)
100	

Table 5: Solution of Pell's equation for $51 \leq N \leq 100$

N	Pell's solutions (P_n, Q_n)
501	(11242731902975,502288218432),
502	(3832352837,171046278),
503	(24648,1099),(1215047807,54176304),(59896996669224,2670675080885),
504	(449,20),(403201,17960),(362074049,16128060),(325142092801,14482979920)
505	(809,36),(1308961,58248),(2117898089,94245228)
506	(45,2),(4049,180),(364365,16198),(32788801,1457640),(2950627725,131171402)
507	(1351,60),(3650401,162120),(9863382151,438048180),(26650854921601,1183606020240),
508	(44757606858751,1985797689600),
509	
510	(271,12),(146881,6504),(79609231,3525156),(43148056321,1910628048)
511	(4188548960,185290497),
512	(665857,29427),(886731088897,39188347878),
513	(13771351,608020),(379300216730401,16746513670040),
514	(4625,204),(42781249,1887000),(395726548625,17454749796),
515	(17406,767),(605937671,26700804),(21093902185446,929508388081),
516	(16855,742),(568182049,25012820),(19153416854935,843182161458),
517	(590968985399,25990786260),
518	(2367,104),(11205377,492336),(53046252351,2330718520)
519	(14851876,651925),(441156441438751,19364618522600),
520	(6499,285),(84474001,3704430),(1097993058499,48150180855),
521	
522	(19603,858),(768555217,33638748),(30131975818099,1318840753230),
523	(81810300626,3577314675),
524	(225144199,9835470),
525	(6049,264),(73180801,3193872),(885341324449,38639463192),
526	
527	(528,23),(557567,24288),(588790224,25648105),(621761918977,27084374592)
528	(23,1),(1057,46),(48599,2115),(2234497,97244),(102738263,4471109)
529	
530	(1059,46),(2242961,97428),(4750590339,206352458),(10061748095041,437054408616),
531	(530,23),(561799,24380),(595506410,25842777),(631236232801,27393319240)
532	(2588599,112230),(13401689565601,581036931540),
533	(74859849,3242540),
534	(3678725,159194),(27066035251249,1171261895300),
535	(1618804,69987),(5241052780831,226590471096),
536	(145925,6303),(42588211249,1839530550),
537	(192349463,8300492),
538	(9536081203,411129654),
539	(3970,171),(31521799,1357740),(250283080090,10780455429),
540	(119071,5124),(28355806081,1220239608),
541	
542	(4293183,184408),(36862840542977,1583394581328),
543	(669337,28724),(896024039137,38452071976),
544	(2449,105),(11995201,514290),(58752492049,2518992315)
545	(1961,84),(7691041,329448),(30164260841,1292094972)
546	(701,30),(982801,42060),(1377886301,58968090),(1931795611201,82673220120),
547	(160177601264642,6848699678673),
548	(6083073,259856),(74007554246657,3161446034976),
549	(1766319049,75384660),
550	(30580901,1303974),

Table 6: $500 \leq N \leq 550$

Question 4

If $x^2 \equiv y^2 \pmod{N}$, then $N|x^2 - y^2 = (x+y)(x-y)$. Now if $d = \gcd(N, x+y)$ is strictly between 1 and N, then d is a non-trivial divisor of N and we get the factorisation $N = d.\frac{N}{d}$. So all we have to do is compute $\gcd(N, x+y)$, if it turns out to be 1 or N, we move on to the next (x, y) pair. Hence it has the same complexity as computing gcd which can be done in$O(n)$ operations.

Now if N is composite, we must have $N = ab$ for some odd $1 < a, b < N$ since N is odd. Then we can write $N = ab = (\frac{a+b}{2})^2 - (\frac{a-b}{2})^2$. So we can just take $x = \frac{a+b}{2}$, $y = \frac{a-b}{2}$, and we have $\gcd(x+y, N) = \gcd(a, N) = a \in [2, n-1]$. So such x, y always exist.

Question 5

A programs to compute $P_n \mod N$ and $P_n^2 \mod N$ for N up to 10^{10} can be found in page 7.

For avoiding integer overflow, we write each integer $b < 10^{10}$ in the form $10^5.u + v$ s.t $0 \le u, v < 10^5$, using division algorithm. Then for any $a < 10^{10}$, we have

$$ab \mod N = \Big(\big(10^5(au \mod N) \mod N\big) + (av \mod N)\Big) \mod N$$

Since MATLAB can do multiplications of two integers less than 10^{10} and 10^5, we are fine.

Table 7 shows the result for $N = 1449774329, 3333999913$ and 7686335197 .

	$P_n \mod N$	$P_n^2 \mod N$	$P_n \mod N$	$P_n^2 \mod N$	$P_n \mod N$	$P_n^2 \mod N$
N / n	1449774329		3333999913		7686335197	
1	38075	1449705625	57740	3333907600	87671	7686204241
2	38076	7447	57741	23168	87672	44387
3	380759	1449757510	230963	3333908674	263015	7686208649
4	1561112	29495	288704	1791	350687	8817
5	3502983	1449751962	18419315	3333922345	6926068	7686311344
6	8567078	52459	18708019	37273	48833163	50516
7	12070061	1449771169	55835353	3333987265	153425557	7686282946
8	286178481	29137	465390843	83849	509109834	6503
9	584427023	1449740329	521226196	3333975752	5703946044	7686221950
10	870605504	37991	2029069431	83408	6213055878	59988
11	5258198	1449753174	2550295627	3333986530	4230666725	7686222176
12	886380098	104	3211139255	86943	2757387406	7181
13	1349759102	1449702004	2427434969	3333980297	6159895487	7686206881
14	786364871	3733	2012314448	93	1230947696	43363
15	343174032	1449744393	2543730100	3333934380	2166403378	7686320746
16	22938606	30305	1222044635	49936	2002379263	143276
17	389051244	1449772441	431774822	3333968626	4168782641	7686314144
18	698193832	69383	2517369101	20899	438516962	68397
19	1087245076	1449769194	3016620588	3333973401	5045816565	7686271596
20	334636530	61336	1247851801	18507	2843814895	45033

Table 7: Values of $P_n \mod N$ and $P_N^2 \mod N$

Question 6

A program using Gaussian elimination to find a non-zero column vector v with $Av = 0$ where A is matrix over field $\mathbb{Z}/2\mathbb{Z}$ can be found in page 16 named `gaussian_elim.m`. Our program always returns a solution with $v_n = 1$ if such a solution exists where n is the dimension of v.

Question 7

A program for continued fraction method can be found in page 8. The program takes a (i) set B of primes, (ii) integer N which needs to be factored and (iii)an integer k indicating how many convergents to be computed

1. At first we choose a factor base B, which consists of first few prime numbers including -1.

2. Then we compute $P_n \mod N$ and $P_n^2 \mod N$ for $n = 1$ to 100/150 as we did in Q5. If $P_n^2 \mod N$ is bigger than $N/2$, we change it to $-(N - P_n^2 \mod N)$. Let it be equal to c_n.

3. For each n, we determine whether c_n is a B-number, construct a vector v consisting of those n's in increasing order.

4. Now starting from $k = 2$, we take the first k B-numbers($P_{v(1)}, \cdots P_{v(k)}$ and construct a $k \times l$ matrix A where the ith row is obtained from the prime factorisation of $P_{v(k)}$. Then we solve $Ax = 0$ in $\mathbb{Z}/2\mathbb{Z}$ using 8. If there exists a non-trivial solution, we find a non-empty subset $I \subseteq \{1, \ldots, v(k)\}$ such that $\prod_{i \in I} c_i = y^2$ for some $y \in \mathbb{Z}$,

5. Then if $x = \prod_{i \in I} P_i \mod N$, we have $x^2 \equiv y^2 \mod N$. If $x \not\equiv \pm y \pmod N$, then Q4 implies we have found a factor s of N where $s = \gcd(x+y, N)$.

6. Otherwise we try with $k+1$. Notice that, 8 always finds a solution with $x_k = 1$ if exists. That way it makes sure that we are always finding different subset I, hence producing different x and y.

as input and prints out

1. All $1 \le n \le k$ s.t $P_n^2 \pmod N$ is a B-number.

2. In the occurrence of existence of an $I \in \{1, \cdots, n\}$ as we mentioned earlier, the program prints out I and x, y where $x = \prod_{i \in I} P_i \pmod N$ and $y = (\prod_{i \in I} c_i)^{1/2}$

3. If $s = \gcd(x+y, N) > 1$, program returns s and $t = N/s$.

We run for different values of N.

1. $N = 1449774329$

```
>> cf_method(1449774329,100)
B_number = 9, 12, 16, 20, 26, 34, 42, 44, 45, 51, 60, 66, 74, 80, 83, ...
    90, 92, 97, 98, 100,

I = 26,
x = 52, y = 52

I = 26, 44,
x = 975934620, y = 7540

N = 51043 * 28403
ans =

        51043
```

Here we get a factorisation in the 2nd try. In the 1st try, we get $I = \{26\}$ which gives $x = y = P_{26} = 52$. This obviously doesn't give a non-trivial factorization.

Now for $I = \{26, 44\}$, we get

$$\begin{aligned} P_{26}P_{44} &\equiv 52.1245500098 \pmod N \\ &\equiv 975934620 \pmod N \end{aligned}$$

and

$$\begin{aligned} (c_{26}c_{44})^{1/2} &\equiv \left[2^{4+0}.5^{0+2}.13^{2+0}.29^{0+2}\right]^{1/2} \pmod N \\ &\equiv (2^2.5.13.29) \pmod N \\ &\equiv 7540 \pmod N \end{aligned}$$

Now $\gcd(N, x+y) = \gcd(1449774329, 975934620 + 7540) = 51043$, so we get $N = 51043 \times 28403$.

2. $N = 3333999913$,

```
>> cf_method(3333999913,200)
B_number = 7, 14, 21, 23, 28, 41, 45, 46, 50, 80, 85, 101, 111, 119, ...
    132, 135, 150, 152, 169, 171, 176, 182, 195, 200,

I = 7, 14, 21,
x = 3333987265, y = 3333987265

I = 7, 14, 21, 28,
x = 3332823649, y = 3332823649

I = 14, 21, 28, 41,
x = 3332823649, y = 3332823649

I = 21, 23, 28, 41, 45,
x = 1398577896, y = 1398577896

I = 21, 23, 28, 41, 45, 50,
x = 1582700549, y = 1751299364

I = 7, 14, 21, 23, 28, 41, 45, 50, 80, 111,
x = 1700129568, y = 1633870345

I = 7, 21, 23, 28, 41, 45, 50, 80, 101, 111, 119,
x = 1666519069, y = 1667480844

I = 7, 21, 23, 28, 41, 45, 46, 50, 101, 111, 119, 132,
x = 1485705369, y = 1848294544

I = 7, 21, 23, 28, 41, 45, 46, 50, 111, 119, 132, 135,
x = 495235123, y = 2838764790

I = 7, 14, 21, 28, 41, 45, 46, 50, 101, 111, 119, 132, 135, 152,
x = 46573696, y = 46573696

I = 14, 21, 23, 28, 41, 45, 50, 111, 119, 132, 135, 152, 169,
x = 2466986593, y = 2772441816

N = 99991 * 33343
ans =

99991
```

Here we succeed in the 10th try. For example in the 5th try, we get $I = \{21, 23, 28, 41, 45, 50\}$. We compute the prime factorisation of $P_i \pmod N$ and $P_i^2 \pmod N$ using `prod_primes.m` to get

$$\begin{aligned} P_{21}P_{23}P_{28}P_{41}P_{45}P_{50} \equiv & 501731655 \times 466038032 \times 93 \times 55835353 \times 245721913 \\ & \times 3333999845 \pmod N \\ \equiv & 1582700549 \pmod N \end{aligned}$$

$$\begin{aligned} (c_{21}c_{23}c_{28}c_{41}c_{45}c_{50})^{1/2} \equiv & \big[(-1)^{1+1+0+1+1+0}.2^{3+0+0+3+0+4}.3^{0+1+2+1+0+0}.17^{1+0+0+1+0+2} \\ & 29^{0+1+0+0+1+0}.31^{0+0+2+1+1+0}.41^{0+1+0+0+1+0}\big]^{1/2} \pmod N \\ \equiv & 2^5.3^2.17^2.29.31^2.41 \pmod N \\ \equiv & 1751299364 \pmod N \end{aligned}$$

We see that they are equivalent $\pmod N$, hence we don't get a factorization.

Now for $I = \{14, 21, 23, 28, 41, 45, 50, 111, 119, 132, 135, 152, 169\}$, we get

$$\begin{aligned}
&P_{14}P_{21}P_{23}P_{28}P_{41}P_{45}P_{50}P_{111}P_{119}P_{132}P_{135}P_{152}P_{169}\\
\equiv &2012314448 \times 501731655 \times 466038032 \times 93 \times 55835353 \times 245721913 \times 3333999845\\
&\times 539271719 \times 987800190 \times 202624337 \times 836809419 \times 1865893194 \times 1696557395 \pmod N\\
\equiv &2466986593 \pmod N
\end{aligned}$$

and

$$\begin{aligned}
&(c_{14}c_{21}c_{23}c_{28}c_{41}c_{45}c_{50}c_{111}c_{119}c_{132}c_{135}c_{152}c_{169})^{1/2}\\
\equiv &[\ (-1)^{0+1+1+0+1+1+0+1+1+0+1+0+1}.2^{0+3+0+0+3+0+4+3+0+0+0+0+5}\\
&3^{1+0+1+2+1+0+0+2+3+1+2+4+1}.13^{0+0+0+0+0+0+0+0+0+1+0+0+1+}\\
&17^{0+1+0+0+1+0+2+1+0+0+0+0+1}29^{0+0+1+0+0+1+0+0+0+1+0+1+0}\\
&31^{1+0+0+2+1+1+0+0+0+0+1+0+0}.37^{0+0+1+0+0+1+0+0+1+0+1+0+0}.\\
&47^{0+0+0+0+0+0+0+1+0+1+0+0+0}\ ]^{1/2} \pmod N\\
\equiv &2^9.3^9.13.17^3.29^2.31^3.37^2.47 \pmod N\\
\equiv &2772441816 \pmod N
\end{aligned}$$

3. $N = 7686335197$

```
>> cf_method(7686335197,200)
B_number = 13, 16, 131, 153,

I = 16, 131, 153,
x = 7393655649, y = 7668282421

N = 93257 * 82421
ans =

93257
```

Here we succeed in the 1st try. We get $I = \{16, 131, 153\}$. We compute the prime factorisation of $P_i \pmod N$ and $P_i^2 \pmod N$ using `prod_primes.m` to get

$$\begin{aligned}
P_{16}P_{131}P_{153} &\equiv (2002379263 \times 1821227876 \times 6615421364) \pmod N\\
&\equiv 7393655649 \pmod N
\end{aligned}$$

$$\begin{aligned}
(c_{16}c_{131}c_{153})^{1/2} &\equiv \left[(-1)^{0+1+1}.2^{2+2+2}.3^{0+0+4}.7^{2+3+1}.17^{1+0+1}.43^{1+1+0}\right]^{1/2} \pmod N\\
&\equiv (-2^3.3^2.7^3.17.43) \pmod N\\
&\equiv 7668282421 \pmod N
\end{aligned}$$

Now $\gcd(N, x + y) = \gcd(7686335197, 7393655649 + 7668282421) = 93257$, so we get $N = 93257 \times 82421$.

Programs

Listing 1: prod_primes.m

```
function [p,C] = prod_primes(B,N)

n = length(B);
C = zeros(1,n);

if n == 0 && N > 1
    p = 0;

elseif n > 0 && N == 1
    p = 1;
    return

elseif B(1) == -1
    if N > 0
        B(1) = [] ;
        [p,C] = prod_primes(B,N);
        C = [0,C];
    else
        B(1) = [] ;
        [p,C] = prod_primes(B,-N);
        C = [1,C];
    end

elseif mod(N,B(1)) == 0
    N = N/B(1);
    [p,C] = prod_primes(B,N);
    C(1) = C(1) + 1;

else
    B = setdiff(B,B(1));
    storeme = C(1);
    [p,C] = prod_primes(B,N);
    C = [storeme,C];
end
end
```

Listing 2: cont_frac.m

```
function [A,max_r,max_s,P,Q,U,V] = cont_frac (N,k)

r = 0;
s = 1;
max_r = 0;
max_s = 1;

p_ = 1;
q_ = 0;

A = zeros(1,k) ;   %%%%%% Partial sequence  %%%%%%
P = zeros(1,k) ;   %%%%%%      p            %%%%%%
Q = zeros(1,k) ;   %%%%%%      q            %%%%%%
U = zeros(1,k) ;   %%%%%%    p^2 - Nq^2     %%%%%%
V = zeros(1,k) ;   %%%%%% is p^2 - Nq^2 = 1 %%%%%%

for i = 1:k
    a = floor((r+sqrt(N))/s);
```

```
    r = s*(a) - r ;
    s = (N - r^2)/s ;

    if i == 1
        p = a ;
        q = 1 ;
    else
        storep = p;
        storeq = q;

        p = a*p + p_ ;
        q = a*q + q_ ;

        p_ = storep;
        q_ = storeq;
    end

    u = p^2 - N*q^2;
    v = is_1(p,q,N);

    A(i) = a ;
    P(i) = p ;
    Q(i) = q ;
    U(i) = u ;
    V(i) = v ;

    if r > max_r
        max_r = r;
    end
    if s > max_s
        max_s = s;
    end
end

end
```

Listing 3: `mod_mult.m`

```
function m = mod_mult(a,b,N)

if abs(b) < 10^5
    m = mod(a*b,N);
else
    u = floor(b/10^5);
    v = b - 10^5*u;
    m = mod( 10^5*(mod(a*u,N)) , N) + mod(a*v,N);
    m = mod(m,N);
end
```

Listing 4: `mod_vmult.m`

```
function m = mod_vmult(v,N)

m = 1;
for i=1:length(v)
    m = mod_mult(m,v(i),N);
end
```

Listing 5: is_1.m

```
function r = is_1(x,y,N)

p(1) = 1009;
p(2) = 1013;
p(3) = 1019;
p(4) = 1021;
p(5) = 1031;

f = @(q,i) mod( mod(x,q)^2 - mod(N,q)*mod(y,q)^2 - i, q) ;

if f(4,1) == 0
    i = 1;
elseif f(4,3) == 0
    i = -1;
else
    r = 0;
    return
end

for j = 1:5
    if f(p(j),i) == 0
        r = i;
    else
        r = 0;
        return
    end
end

end
```

Listing 6: pell_solution.m

```
function [Pell,N_Pell] = pell_solution (N,k)

[~,~,~,P,Q,~,V] = cont_frac (N,k);

Pell = zeros(0,3);
N_Pell = zeros(0,3);

for i = 1:k
    if V(i) == 1 && P(i) < 10^15
        Pell = [Pell; i,P(i),Q(i)];

    elseif V(i) == -1 && P(i) < 10^15
        N_Pell = [N_Pell; i,P(i),Q(i)];

    end
end
```

Listing 7: cont_frac2.m

```
function [ PmodN , P_squaremodN ] = cont_frac2 (N,k)

r = 0;
s = 1;

pmodN_ = 1;

PmodN = zeros(1,k);
```

```
P_squaremodN = zeros(1,k);

for i = 1:k
    a = floor((r+sqrt(N))/s);
    r = s*(a) - r;
    s = (N - r^2)/s ;

    if i == 1

        pmodN = mod(a,N);
        p_squaremodN = mod_mult(pmodN,pmodN,N);

    else

        storepmodN = pmodN;
        pmodN = mod( mod_mult(a,pmodN,N) + pmodN_, N) ;
        pmodN_ = storepmodN;

        p_squaremodN = mod_mult(pmodN,pmodN,N);

    end

    PmodN(i) = pmodN ;
    P_squaremodN(i) = p_squaremodN ;

end
end
```

Listing 8: gaussian_elim.m

```
function [p,x] = gaussian_elim ( A )

A = mod(A,2);

[m,n] = size(A);
x = zeros(1,n);
p = 0;

if  n == 1
    if  A == 0
        x = 1;
        p = 1;
    end

elseif m == 1
    t = sum(A) ;
    if  t == 0
        p = 0;
    elseif t == 1
        p = 1;
        if A(1,n) == 1
            x(n-1) = 1;
        else
            x(n) = 1;
        end
    else
        p = 1;
        x(n) = 1;
        s = find(A(1,:));
        x(s(t)) = 1;
        x(s(t-1)) = 1;
    end
```

```
elseif sum(A(:,1)) == 0
    x(1) = 1;
    [~,x(2:n)] = gaussian_elim ( A(:, 2:n) );
    p = 1;

else
    i = 1;
    while A(i,1) == 0
        i = i + 1 ;
    end
    A([1 i], :) = A([i 1], :);

    for k = 2:m
            A(k,:) = mod(A(k,1)*A(1,:) + A(k,:) , 2) ;
    end

    [p,y] = gaussian_elim ( A(2:m,2:n) ) ;
    x(1) = dot(A(1,2:n) , y );
    x = [ mod(x(1),2)  y ] ;
end
end
```

Listing 9: cf_method.m

```
function [s,t] = cf_method(N,k)

B = [-1 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 ] ;

r = length(B);
[ PmodN , P_squaremodN ] = cont_frac2 (N,k);

for i = 1:k
    if P_squaremodN(i) > N/2
        P_squaremodN(i) = -(N - P_squaremodN(i)) ;
    end
end

B_number = [];
for i = 1:k
    if prod_primes(B, P_squaremodN(i) ) == 1
        B_number = [B_number,i];
    end
end

fprintf('B_number = ')
fprintf('%d, ',B_number)
fprintf('\n')

for j=2:length(B_number)
    A = zeros(r,j);
    for i = 1:j
        [~,A(:,i)] = prod_primes(B, P_squaremodN(B_number(i)));
    end

    %[~,b] = prod_primes(B, P_squaremodN(v(j+1)));

    [~,x] = gaussian_elim ( A );

    if x(j) == 1

        y = zeros(r,1);
```

```
        for i = 1:j
            if x(i) == 1
                y = y + A(:,i)/2;
            end
        end

        C_prod = 1;
        for l = 1:r
            C_prod = mod_mult(C_prod, B(l)^(y(l)) ,N);
        end

        P_prod = 1;
        for i = 1:j
            if x(i) == 1
                P_prod = mod_mult(P_prod, PmodN(B_number(i)), N);
            end
        end

        n = B_number(find(x)) ;
        fprintf('\n I = ')
        fprintf('%d, ',n)
        fprintf('\n x = %d, y = %d \n', P_prod, C_prod);

        if P_prod ~= C_prod && P_prod + C_prod ~= N

            s = gcd(P_prod + C_prod,N);
            t = N/s;
            fprintf('\n N = %d * %d', s , t)

            return
        else

        end
    end
end
end
```