3. Dviejų pirminių skaičių sandaugos skaidymas naudojant standartinius elementus

Eilė	pq	p	q	Radimo laikas, s	Visiško perrinkimo laikas, s
21	2949300426067	1627837	1811791	0,0080	0,1379
21	1879730985789	1253093	1500073	0,0156	0,1021
21	2882839800611	1497997	1924463	0,0156	0,1248
22	11016803125121	2793883	3943187	0,0156	0,0863
22	9085815241199	2310019	3933221	0,0156	0,0587
22	14618595213051	3652829	4001719	0,0156	0,1001
23	35614161976277	4390523	8111599	0,0313	0,1153
23	38192326112669	5867107	6509567	0,0153	0,2360
23	61233834512549	7558597	8101217	0,0156	0,4112
24	156799279965739	11879177	13199507	0,0156	0,2789
24	170293931344631	10524959	16180009	0,0201	0,1107
24	173947242148621	10970119	15856459	0,0310	0,1772
25	541916350105979	17223181	31464359	0,0378	0,1442
25	745803302501729	24293029	30700301	0,0156	0,1382
25	510891988702453	21209873	24087461	0,0156	0,2561
26	2383917530698999	39322999	60624001	0,0690	0,3521
26	2454308816196383	45119213	54396091	0,0469	0,5208
26	3404667046545521	58015049	58685929	0,0156	2,6014
27	6105724356316279	67936483	89874013	0,0820	0,6256
27	7624274315888591	85806011	88854781	0,0221	1,2289
27	11087339892589481	82691099	134081419	0,1628	0,7571
28	29998677660068563	150314167	199573189	0,1694	1,2830
28	33983025470131093	142820807	237941699	0,3004	1,3353
28	40086804277328563	151160329	265193947	0,3790	1,5470
29	149718749045031347	283848029	527460943	0,7487	2,8147
29	106145065204577279	314730487	337257017	0,0810	2,3819
29	160128106099418503	308583707	518913029	0,6642	2,9131
30	481414375401836413	559036169	861150677	0,9492	4,8926
30	579549452465685631	602304847	962219473	1,1721	5,6350
30	432290565168968789	582314521	742366109	0,5327	4,6725

4. Dviejų pirminių skaičių sandaugos skaidymas naudojant BigInteger objektus.

Eilė	pq	p	q	Radimo laikas, s	Visiško perrinkimo laikas, s
28	36859888975920757	167069321	220626317	6,3758	48,9409
28	59051715344359271	226504337	260708983	4,2089	61,6127
28	59631777459456269	237243821	251352289	2,2436	78,2380
29	151400081968084549	347231561	436020509	11,3084	105,0143
29	160470126313751753	365272367	439316359	8,7375	98,8518
29	193111764642253949	398419717	484694297	10,0520	107,4657
30	387418007832708301	604763063	640611227	4,2478	149,3690
30	525527638911801259	635607607	826811437	18,7976	152,4208
30	736990825663545833	689310239	1069171447	30,4543	154,5036
31	1797785169055376551	1262550089	1423931759	17,0882	292,6155
31	3041613553744077083	1458381139	2085609497	49,2160	300,4293
31	1915637023447966219	1222720171	1566701089	30,5560	262,0164
32	7351299219915835787	2402880313	3059369699	254,7682	2239,0698
32	8983292752343523707	2347423649	3826873243	105,4945	486,5931
32	6815435062783255963	2217133907	3073984409	65,7679	436,2134

5. Dviejų pirminių skaičių sandaugos skaidymo trukmės nustatymas, naudojant BigInteger objektus.

Eilė	pq	Visiško perrinkimo laikas, s
33	50046785277642375517	2689,693363
33	63641634526744736261	3141,945199
33	59544716706929352413	2926,105441
34	134736731837423358697	4395,074166
34	201764623453222753657	11853,76133
34	290676422269494227107	7301,932481
35	703891519264984516951	9973,021658
35	1120636926536442023641	10549,5918
35	735395123086530368983	8676,9513
36	2903448032897045159701	16972,8834
36	2090416078623524017989	14526,4940
36	3757040723978442836911	19257,8317
37	10756066749103152503217	32622,5849
37	7672100046180702825887	27553,0853
37	10074003095811822301649	38588,3641
38	48147095606362878541789	69785,0899
38	61040271597666109010287	77812,9073
38	54149666913355714785921	73651,4794
39	115957441916780663361431	107935,0212
39	175863334943437185691717	254083,4684
39	247104245010705172166341	191736,9480
40	802417747911654895175353	283911,9285
40	477243766641016083743959	155123,7843
40	495598895781957366860093	492689,3613

1 lentelės suvestinė

Eilė	Vidutinis radimo laikas	Vidutinis visiško perrinkimo laikas
21	0,0131	0,1216
22	0,0156	0,0817
23	0,0207	0,2542
24	0,0223	0,1889
25	0,0230	0,1795
26	0,0438	1,1581
27	0,0890	0,8705
28	0,2829	1,3884
29	0,4980	2,7032
30	0,8846	5,0667

2 lentelės suvestinė

Eilė	Vidutinis radimo laikas	Vidutinis visiško perrinkimo laikas
28	4,2761	62,9305
29	10,0326	103,7773
30	17,8333	152,0978
31	32,2867	285,0204
32	142,0102	1053,9588

3 lentelės suvestinė

Eilė	Vidutinis visiško perrinkimo laikas
28	62,9305
29	103,7773
30	152,0978
31	285,0204
32	1053,9588
33	2915,8193
34	9577,8469
35	9733,1883
36	16919,0697
37	32921,3448
38	73749,8255
39	184585,1458
40	310575,0247

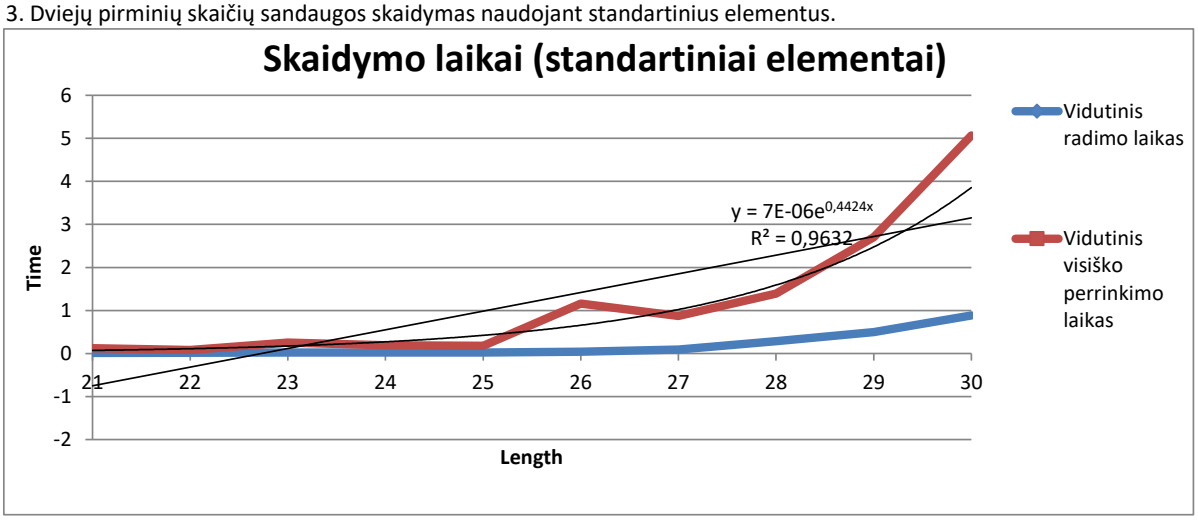
1. Kiek yra pirminių skaičių mažesnių už 10? **4**

2. Kiek yra pirminių skaičių mažesnių už 100? **25**

Išvardykite:

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**		

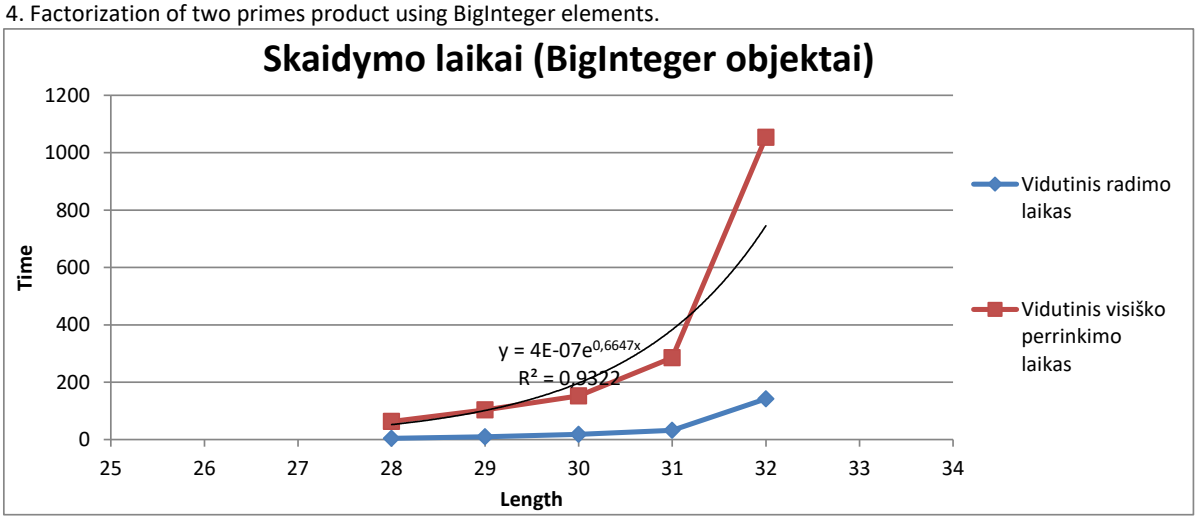
3. Dviejų pirminių skaičių sandaugos skaidymas naudojant standartinius elementus.



Comment:

Vidutinis visiško perrinkimo laikas auga eksponentiškai.

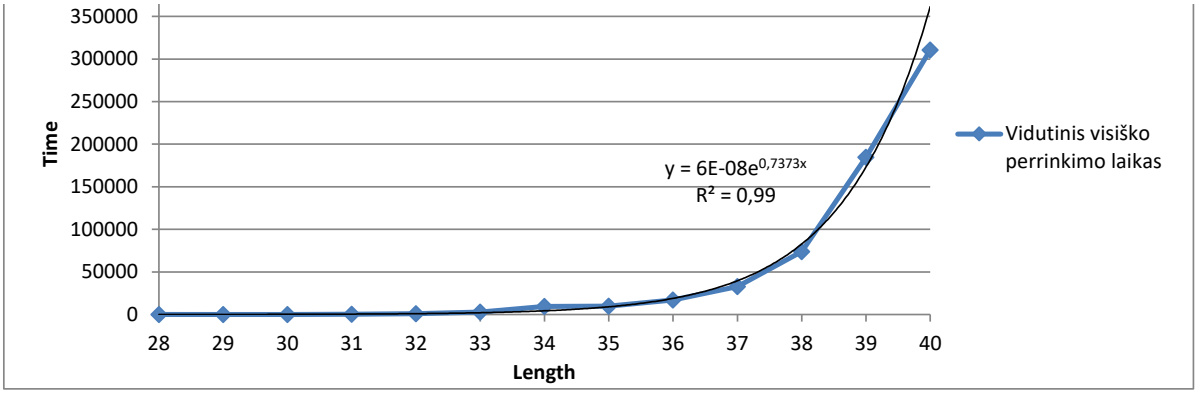
4. Factorization of two primes product using BigInteger elements.



Comment:

Vidutinis visiško perrinkimo laikas ženkliai išauga skaidant 32 bitų pirminius skaičius.

5. Factorization of two primes product using BigInteger elements.



Comment:

Iš grafiko galima matyti, kad vidutinis visiško perrinkimo laikas auga eksponentiškai.

6. Ar skiriasi 3 ir 5 punktuose gautos vidutinės visiško perrinkimo trukmės aproksimacija priklausomai nuo skaičių eilės? Pabandykite paaiškinti kodėl?

Answer:	Dėl skaičiaus dydžio aproksimacija skiriasi. Nuo dydžio ir priklausys, kiek laiko trunka apskaičiuoti pirminių skaičių sandaugos skaidymo trukmę. Tą galima matyti ir grafikuose išreikštose formulėse, nes jos skiriasi.

7. Pabandykite nustatyti kiek užtruktų dviejų 60 bitų ilgio pirminių skaičių sandaugos išskaidymas?

Answer:	Apie 50 metų
Komentaras:	Į 5 užduoties formulę vietoj x įrašiau 60

8. Pabandykite nustatyti kiek užtruktų dviejų 1024 bitų ilgio pirminių skaičių sandaugos išskaidymas?

Answer:	Apie milijoną metų.
Comment:	Į 5 užduoties formulę vietoj x įrašiau 1024.

9. Kiek kartų pagreitėtų išskaidymas, jei tikrinimą galėtume atlikti iš karto su 2 kompiuteriais?

Answer:	2
Komentaras:	Išskaidymo procesas tektų 2 kompiuteriams, todėl darbas būtų atliktas dvigubai greičiau.

10. Kiek kartų pagreitėtų išskaidymas, jei tikrinimą galėtume atlikti iš karto su 100 kompiuterių?

Answer:	100
Comment:	Atsakymas toks pats, kaip 9 klausime; 100 kartų.