

Talnafræði

Frumtölur

Bergur Snorrason

14. mars 2021

- ▶ Heiltala a kallast *samsett* ef til eru heiltölur x og y , báðar stærri en 1, þannig að $a = x \cdot y$.

- ▶ Heiltala a kallast *samsett* ef til eru heiltölur x og y , báðar stærri en 1, þannig að $a = x \cdot y$.
- ▶ Heiltala kallast *frumtala* ef hún er ekki samsett.

- ▶ Heiltala a kallast *samsett* ef til eru heiltölur x og y , báðar stærri en 1, þannig að $a = x \cdot y$.
- ▶ Heiltala kallast *frumtala* ef hún er ekki samsett.
- ▶ Við segjum að talna runa $(a_n)_{n \in \mathbb{N}}$ sé á *endanum núll* ef til er jákvæð heiltala N þannig að $a_n = 0$ fyrir öll $n > N$.

- ▶ Heiltala a kallast *samsett* ef til eru heiltölur x og y , báðar stærri en 1, þannig að $a = x \cdot y$.
- ▶ Heiltala kallast *frumtala* ef hún er ekki samsett.
- ▶ Við segjum að talna runa $(a_n)_{n \in \mathbb{N}}$ sé á *endanum núll* ef til er jákvæð heiltala N þannig að $a_n = 0$ fyrir öll $n > N$.
- ▶ Látum p_n tákna n -tu minnstu jákvæðu frumtöluna.

- ▶ Heiltala a kallast *samsett* ef til eru heiltölur x og y , báðar stærri en 1, þannig að $a = x \cdot y$.
- ▶ Heiltala kallast *frumtala* ef hún er ekki samsett.
- ▶ Við segjum að talna runa $(a_n)_{n \in \mathbb{N}}$ sé á endanum núll ef til er jákvæð heiltala N þannig að $a_n = 0$ fyrir öll $n > N$.
- ▶ Látum p_n tákna n -tu minnstu jákvæðu frumtöluna.
- ▶ Þá er til, fyrir sérhverja jákvæða heiltölu a , nákvæmlega eina runa af jákvæðum heiltölum, $(e_n)_{n \in \mathbb{N}}$, sem er á endanum núll, þannig að

$$a = \prod_{n \in \mathbb{N}} p_n^{e_n}.$$

- ▶ Heiltala a kallast *samsett* ef til eru heiltölur x og y , báðar stærri en 1, þannig að $a = x \cdot y$.
- ▶ Heiltala kallast *frumtala* ef hún er ekki samsett.
- ▶ Við segjum að talna runa $(a_n)_{n \in \mathbb{N}}$ sé á endanum núll ef til er jákvæð heiltala N þannig að $a_n = 0$ fyrir öll $n > N$.
- ▶ Látum p_n tákna n -tu minnstu jákvæðu frumtöluna.
- ▶ Þá er til, fyrir sérhverja jákvæða heiltölu a , nákvæmlega eina runa af jákvæðum heiltölum, $(e_n)_{n \in \mathbb{N}}$, sem er á endanum núll, þannig að

$$a = \prod_{n \in \mathbb{N}} p_n^{e_n}.$$

- ▶ Við köllum þessa þáttun *frumþáttun* tölunnar a .

- ▶ Við þurfum oft að ákvarða hvort tala sé framtala.

- ▶ Við þurfum oft að ákvarða hvort tala sé framtala.
- ▶ Oft þurfum við líka að frumpátta tölur.

- ▶ Við þurfum oft að ákvarða hvort tala sé framtala.
- ▶ Oft þurfum við líka að frumpátta tölur.
- ▶ Til að ákvarða hvort tala sé framtala er yfirleitt farið eina af þremur leiðum.

- ▶ Við þurfum oft að ákvarða hvort tala sé framtala.
- ▶ Oft þurfum við líka að frumpátta tölur.
- ▶ Til að ákvarða hvort tala sé framtala er yfirleitt farið eina af þremur leiðum.
- ▶ Fyrst skoðum við hvernig þetta er gert með tæmandi leit.

- ▶ Við þurfum oft að ákvarða hvort tala sé frumtala.
- ▶ Oft þurfum við líka að frumpátta tölur.
- ▶ Til að ákvarða hvort tala sé frumtala er yfirleitt farið eina af þremur leiðum.
- ▶ Fyrst skoðum við hvernig þetta er gert með tæmandi leit.
- ▶ Síðan skoðum við sigti Eratosþenesar.

- ▶ Við þurfum oft að ákvarða hvort tala sé frumtala.
- ▶ Oft þurfum við líka að frumþátta tölur.
- ▶ Til að ákvarða hvort tala sé frumtala er yfirleitt farið eina af þremur leiðum.
- ▶ Fyrst skoðum við hvernig þetta er gert með tæmandi leit.
- ▶ Síðan skoðum við sigti Eratosþenesar.
- ▶ Að lokum skoðum við slembið reinkirit.

- ▶ Ef n er samsett þá er til tala á milli núll og n sem deilir n .

- ▶ Ef n er samsett þá er til tala á milli núll og n sem deilir n .
- ▶ Köllum þá tölu a .

- ▶ Ef n er samsett þá er til tala á milli núll og n sem deilir n .
- ▶ Köllum þá tölu a .
- ▶ Þá deilir n/a líka n .

- ▶ Ef n er samsett þá er til tala á milli núll og n sem deilir n .
- ▶ Köllum þá tölu a .
- ▶ Þá deilir n/a líka n .
- ▶ Einnig höfum við að $\min(a, n/a) \leq \sqrt{n}$.

- ▶ Ef n er samsett þá er til tala á milli núll og n sem deilir n .
- ▶ Köllum þá tölu a .
- ▶ Þá deilir n/a líka n .
- ▶ Einnig höfum við að $\min(a, n/a) \leq \sqrt{n}$.
- ▶ Við getum því umorðað fyrsta punkt þessara glæru sem „Ef n er samsett þá er til tala á milli núll og \sqrt{n} sem deilir n “.

- ▶ Ef n er samsett þá er til tala á milli núll og n sem deilir n .
- ▶ Köllum þá tölu a .
- ▶ Þá deilir n/a líka n .
- ▶ Einnig höfum við að $\min(a, n/a) \leq \sqrt{n}$.
- ▶ Við getum því umorðað fyrsta punkt þessara glæru sem „Ef n er samsett þá er til tala á milli núll og \sqrt{n} sem deilir n “.

```
4 int isp(ll x)
5 {
6     ll i;
7     if (x <= 1) return 0;
8     for (i = 2; i*i <= x; i++) if (x%i == 0) return 0;
9     return 1;
10 }
```

- ▶ Þetta reiknirit er $\mathcal{O}(\sqrt{n})$ því við þurfum bara að skoða jákvæðar heiltölur minni en \sqrt{n} .

- ▶ Þetta reiknirit er $\mathcal{O}(\sqrt{n})$ því við þurfum bara að skoða jákvæðar heiltölur minni en \sqrt{n} .

- ▶ Þetta reiknirit er $\mathcal{O}(\sqrt{n})$ því við þurfum bara að skoða jákvæðar heiltölur minni en \sqrt{n} .
- ▶ Ef við viljum finna allar framtölur minni en n með þessari aðferð þarf $\mathcal{O}(\quad)$ tíma.

- ▶ Þetta reiknirit er $\mathcal{O}(\sqrt{n})$ því við þurfum bara að skoða jákvæðar heiltölur minni en \sqrt{n} .
- ▶ Ef við viljum finna allar framtölur minni en n með þessari aðferð þarf $\mathcal{O}(n\sqrt{n})$ tíma.

- ▶ Þetta reiknirit er $\mathcal{O}(\sqrt{n})$ því við þurfum bara að skoða jákvæðar heiltölur minni en \sqrt{n} .
- ▶ Ef við viljum finna allar framtölur minni en n með þessari aðferð þarf $\mathcal{O}(n\sqrt{n})$ tíma.
- ▶ Við getum bætt þetta með sigti Eratosþenesar.

Sigti Eratosþenesar

- ▶ Við byrjum á að merkja allar tölur sem „óséðar”.

Sigti Eratosþenesar

- ▶ Við byrjum á að merkja allar tölur sem „óséðar”.
- ▶ Við merkjum síðan 0 og 1 sem „samsettar”.

Sigti Eratosþenesar

- ▶ Við byrjum á að merkja allar tölur sem „óséðar”.
- ▶ Við merkjum síðan 0 og 1 sem „samsettar”.
- ▶ Við endurtökum svo eftir farandi skref þangað til engin óséð tala er eftir:

Sigti Eratosþenesar

- ▶ Við byrjum á að merkja allar tölur sem „óséðar”.
- ▶ Við merkjum síðan 0 og 1 sem „samsettar”.
- ▶ Við endurtökum svo eftir farandi skref þangað til engin óséð tala er eftir:
 - ▶ Látum x vera minnstu „óséðu” töluna.

Sigti Eratosþenesar

- ▶ Við byrjum á að merkja allar tölur sem „óséðar”.
- ▶ Við merkjum síðan 0 og 1 sem „samsettar”.
- ▶ Við endurtökum svo eftir farandi skref þangað til engin óséð tala er eftir:
 - ▶ Látum x vera minnstu „óséðu” töluna.
 - ▶ Merkjum x sem „frumtölu”.

Sigti Eratosþenesar

- ▶ Við byrjum á að merkja allar tölur sem „óséðar”.
- ▶ Við merkjum síðan 0 og 1 sem „samsettar”.
- ▶ Við endurtökum svo eftir farandi skref þangað til engin óséð tala er eftir:
 - ▶ Látum x vera minnstu „óséðu” töluna.
 - ▶ Merkjum x sem „frumtölu”.
 - ▶ Merkjum svo allar tölur á forminu $n \cdot x$, fyrir $n > 1$ sem „samsettar”.

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

		2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

		2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

		2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49
51		53	55	57	59
61		63	65	67	69
71		73	75	77	79
81		83	85	87	89
91		93	95	97	99

	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49
51		53	55	57	59
61		63	65	67	69
71		73	75	77	79
81		83	85	87	89
91		93	95	97	99

	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49
51		53	55	57	59
61		63	65	67	69
71		73	75	77	79
81		83	85	87	89
91		93	95	97	99

	2	3	5	7	
11		13		17	19
		23	25		29
31			35	37	
41		43		47	49
		53	55		59
61			65	67	
71		73		77	79
		83	85		89
91			95	97	

	2	3	5	7	
11		13		17	19
		23	25		29
31			35	37	
41		43		47	49
		53	55		59
61			65	67	
71		73		77	79
		83	85		89
91			95	97	

	2	3	5	7	
11		13		17	19
		23	25		29
31			35	37	
41		43		47	49
		53	55		59
61			65	67	
71		73		77	79
		83	85		89
91			95	97	

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	49
		53			59
61				67	
71		73		77	79
		83			89
91				97	

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	49
		53			59
61				67	
71		73		77	79
		83			89
91				97	

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	49
		53			59
61				67	
71		73		77	79
		83			89
91				97	

	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	

	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	

```
5 int e[MAXN];
6 void eratos()
7 {
8     int i, j;
9     rep(i, MAXN) e[i] = 1;
10    e[0] = e[1] = 0;
11    rep(i, MAXN) if (e[i] == 1) for (j = 2*i; j < MAXN; j += i) e[j] = 0;
12 }
13
14 int isp(int x)
15 {
16     return e[x] == 1;
17 }
```

► Pað tekur $\mathcal{O}(\quad)$ tíma að forreikna sigtið.

- ▶ Það tekur $\mathcal{O}(n \log \log n)$ tíma að forreikna sigtið.

- ▶ Það tekur $\mathcal{O}(n \log \log n)$ tíma að forreikna sigtið.
- ▶ Hver fyrirspurn er síðan afgreidd í $\mathcal{O}()$ tíma.

- ▶ Það tekur $\mathcal{O}(n \log \log n)$ tíma að forreikna sigtið.
- ▶ Hver fyrirspurn er síðan afgreidd í $\mathcal{O}(1)$ tíma.

Slembin reiknirit

- ▶ Hingað til hafa reinkiritin okkar verið annað hvort rétt eða röng.

Slembin reiknirit

- ▶ Hingað til hafa reinkiritin okkar verið annað hvort rétt eða röng.
- ▶ Það er þó til flokkur reinkirit þar á milli.

Slembin reiknirit

- ▶ Hingað til hafa reinkiritin okkar verið annað hvort rétt eða röng.
- ▶ Það er þó til flokkur reinkirit þar á milli.
- ▶ *Slembið reiknirit* er reiknirit sem skilar réttu svar með líka p .

Slembin reiknirit

- ▶ Hingað til hafa reinkiritin okkar verið annað hvort rétt eða röng.
- ▶ Það er þó til flokkur reinkirit þar á milli.
- ▶ *Slembið reiknirit* er reiknirit sem skilar réttu svar með líka p .
- ▶ Við getum þá keyrt reikniritið s sinnum, og þá er það rétt með líkum p^s .

Slembin reiknirit

- ▶ Hingað til hafa reinkiritin okkar verið annað hvort rétt eða röng.
- ▶ Það er þó til flokkur reinkirit þar á milli.
- ▶ *Slembið reiknirit* er reiknirit sem skilar réttu svar með líka p .
- ▶ Við getum þá keyrt reikniritið s sinnum, og þá er það rétt með líkum p^s .
- ▶ Ef reikniritið hefur tímaflækju $\mathcal{O}(f(n))$ þá tekur það $\mathcal{O}(s \cdot f(n))$ að keyra það s sinnum.

Slembin reiknirit

- ▶ Hingað til hafa reinkiritin okkar verið annað hvort rétt eða röng.
- ▶ Það er þó til flokkur reinkirit þar á milli.
- ▶ *Slembið reiknirit* er reiknirit sem skilar réttu svar með líka p .
- ▶ Við getum þá keyrt reikniritið s sinnum, og þá er það rétt með líkum p^s .
- ▶ Ef reikniritið hefur tímaflækju $\mathcal{O}(f(n))$ þá tekur það $\mathcal{O}(s \cdot f(n))$ að keyra það s sinnum.
- ▶ Ef $p = 1/2$, til dæmis, þá fæst fyrir $s = 20$ að líkurnar eru betri en 10^{-6} .

Reiknirit Millers og Rabins

- ▶ Til er slembið reiknirit, kennt við Miller og Rabin, sem ákvarðar hvort tala sé samsett.

Reiknirit Millers og Rabins

- ▶ Til er slembið reiknirit, kennt við Miller og Rabin, sem ákvarðar hvort tala sé samsett.
- ▶ Í því eru líkur á röngu svar minni eða jafnar $1/4$.

Reiknirit Millers og Rabins

- ▶ Til er slembið reiknirit, kennt við Miller og Rabin, sem ákvarðar hvort tala sé samsett.
- ▶ Í því eru líkur á röngu svar minni eða jafnar $1/4$.
- ▶ Tímaflækjan á reikniritinu er $\mathcal{O}(s \cdot \log^3 n)$ og það er rétt með líkum betri en $1/4^s$.

Reiknirit Millers og Rabins

- ▶ Til er slembið reiknirit, kennt við Miller og Rabin, sem ákvarðar hvort tala sé samsett.
- ▶ Í því eru líkur á röngu svar minni eða jafnar $1/4$.
- ▶ Tímaflækjan á reikniritinu er $\mathcal{O}(s \cdot \log^3 n)$ og það er rétt með líkum betri en $1/4^s$.
- ▶ Ég mun ekki fara í það afhverju reikniritið virkar.

Reiknirit Millers og Rabins

- ▶ Til er slembið reiknirit, kennt við Miller og Rabin, sem ákvarðar hvort tala sé samsett.
- ▶ Í því eru líkur á röngu svar minni eða jafnar $1/4$.
- ▶ Tímaflækjan á reikniritinu er $\mathcal{O}(s \cdot \log^3 n)$ og það er rétt með líkum betri en $1/4^s$.
- ▶ Ég mun ekki fara í það afhverju reikniritið virkar.
- ▶ Það er þó gott að þekkja það nógu vel til að geta notað það.

Reiknirit Millers og Rabins

- ▶ Til er slembið reiknirit, kennt við Miller og Rabin, sem ákvarðar hvort tala sé samsett.
- ▶ Í því eru líkur á röngu svar minni eða jafnar $1/4$.
- ▶ Tímaflækjan á reikniritinu er $\mathcal{O}(s \cdot \log^3 n)$ og það er rétt með líkum betri en $1/4^s$.
- ▶ Ég mun ekki fara í það afhverju reikniritið virkar.
- ▶ Það er þó gott að þekkja það nógu vel til að geta notað það.
- ▶ Útfærslan sem er gefin notar niðurstöðu Jiang og Deng (2014) til að virka alltaf fyrir nógu litlar tölur.

```

27 int miller_rabin(ll n)
28 {
29     if (n%2 == 0) return n == 2;
30     if (n <= 3) return n == 3;
31     ll i, k, s = 0, d = n - 1,
32     t[12] = {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37};
33     while (d%2 == 0) d /= 2, s++;
34     rep(k, 12) if (t[k] <= n - 2)
35     {
36         ll a = t[k];
37         ll x = modpow(a, d, n);
38         if (x == 1 || x == n - 1) continue;
39         rep(i, s - 1) if ((x = bigprod(x, x, n)) == n - 1) break;
40         if (i == s - 1) return 0;
41     }
42     return 1;
43 }

```

- ▶ Þegar kemur að því að frumbátta tölur hafa þessar þrjár aðferðir sér hliðstæðu.

- ▶ Þegar kemur að því að frumþátta tölur hafa þessar þrjár aðferðir sér hliðstæðu.
- ▶ Skoðum aftur fyrstu aðferðina.

- ▶ Þegar kemur að því að frumþátta tölur hafa þessar þrjár aðferðir sér hliðstæðu.
- ▶ Skoðum aftur fyrstu aðferðina.

```
4 int isp( ll x)
5 {
6     ll i;
7     if (x <= 1) return 0;
8     for (i = 2; i*i <= x; i++) if (x%i == 0) return 0;
9     return 1;
10 }
```

- ▶ Þegar kemur að því að frumþátta tölur hafa þessar þrjár aðferðir sér hliðstæðu.
- ▶ Skoðum aftur fyrstu aðferðina.

```
4 int isp(int x)
5 {
6     int i;
7     if (x <= 1) return 0;
8     for (i = 2; i*i <= x; i++) if (x%i == 0) return 0;
9     return 1;
10 }
```

- ▶ Þegar þetta fall skilar núll er i minnsti frumþáttur x .

- ▶ Þegar kemur að því að frumþátta tölur hafa þessar þrjár aðferðir sér hliðstæðu.
- ▶ Skoðum aftur fyrstu aðferðina.

```
4 int isp( ll x)
5 {
6     ll i;
7     if (x <= 1) return 0;
8     for (i = 2; i*i <= x; i++) if (x%i == 0) return 0;
9     return 1;
10 }
```

- ▶ Þegar þetta fall skilar núll er i minnsti frumþáttur x .
- ▶ Við getum nú stytt x með i þar til i gengur ekki lengur upp í x .

- ▶ Þegar kemur að því að frumþátta tölur hafa þessar þrjár aðferðir sér hliðstæðu.
- ▶ Skoðum aftur fyrstu aðferðina.

```
4 int isp(II x)
5 {
6     II i;
7     if (x <= 1) return 0;
8     for (i = 2; i*i <= x; i++) if (x%i == 0) return 0;
9     return 1;
10 }
```

- ▶ Þegar þetta fall skilar núll er i minnsti frumþáttur x .
- ▶ Við getum nú stytt x með i þar til i gengur ekki lengur upp í x .
- ▶ Svo höldum við áfram.

```
4 int factor(ll x)
5 {
6     ll i;
7     for (i = 2; i*i <= x;)
8     {
9         if (x%i == 0) printf("%lld ", i), x /= i;
10        else i++;
11    }
12    if (x != 1) printf("%lld ", x);
13    printf("\n");
14    return 1;
15 }
```

```

4 int factor(ll x)
5 {
6     ll i;
7     for (i = 2; i*i <= x;)
8     {
9         if (x%i == 0) printf("%lld ", i), x /= i;
10        else i++;
11    }
12    if (x != 1) printf("%lld ", x);
13    printf("\n");
14    return 1;
15 }

```

► Tímaflækja þessarar aðferðar er $\mathcal{O}(\quad)$.

```

4 int factor(ll x)
5 {
6     ll i;
7     for (i = 2; i*i <= x;)
8     {
9         if (x%i == 0) printf("%lld ", i), x /= i;
10        else i++;
11    }
12    if (x != 1) printf("%lld ", x);
13    printf("\n");
14    return 1;
15 }

```

► Tímaflækja þessarar aðferðar er $\mathcal{O}(\sqrt{n})$.

- ▶ Í stað þess að láta sigti Eratosþenesar geyma hvort tala sé samsett eða ekki getum við látið það geyma minnsta frumþátt tölunnar.

- ▶ Í stað þess að láta sigti Eratosþenesar geyma hvort tala sé samsett eða ekki getum við látið það geyma minnsta frumþátt tölunnar.
- ▶ Takið eftir að n er frumtala þá og því aðeins að minnsti frumþáttur x sé x .

- ▶ Í stað þess að láta sigti Eratosþenesar geyma hvort tala sé samsett eða ekki getum við látið það geyma minnsta frumþátt tölunnar.
- ▶ Takið eftir að n er frumtala þá og því aðeins að minnsta frumþáttur x sé x .
- ▶ Til að þátta tölur förum við endurkvæmt í gegn líkt og þegar við útfærðum sammengisleit.

```

5  int e[MAXN];
6  void eratos()
7  {
8      int i, j;
9      rep(i, MAXN) e[i] = 0;
10     e[0] = e[1] = -1;
11     rep(i, MAXN) if (e[i] == 0)
12         for (j = i; j < MAXN; j += i) if (e[j] == 0) e[j] = i;
13 }
14
15 void factor(int x)
16 {
17     if (x < 2) return;
18     printf("%d ", e[x]);
19     factor(x/e[x]);
20 }
21
22 int isp(int x)
23 {
24     return e[x] == x;
25 }

```

- ▶ Þessi útgáfa er ekki verri en hin á neinn veg, og því er sniðugt að nota hana alltaf.

- ▶ Þessi útgáfa er ekki verri en hin á neinn veg, og því er sniðugt að nota hana alltaf.
- ▶ Hún hefur sömu tímaflækjur: $\mathcal{O}(\quad)$ tíma að forreikna og $\text{isp}(\dots)$ fyrirspurnin tekur $\mathcal{O}(\quad)$ tíma.

- ▶ Þessi útgáfa er ekki verri en hin á neinn veg, og því er sniðugt að nota hana alltaf.
- ▶ Hún hefur sömu tímaflækjur: $\mathcal{O}(n \log \log n)$ tíma að forreikna og $\text{isp}(\dots)$ fyrirspurnin tekur $\mathcal{O}(\quad)$ tíma.

- ▶ Þessi útgáfa er ekki verri en hin á neinn veg, og því er sniðugt að nota hana alltaf.
- ▶ Hún hefur sömu tímaflækjur: $\mathcal{O}(n \log \log n)$ tíma að forreikna og $\text{isp}(\dots)$ fyrirspurnin tekur $\mathcal{O}(1)$ tíma.

- ▶ Þessi útgáfa er ekki verri en hin á neinn veg, og því er sniðugt að nota hana alltaf.
- ▶ Hún hefur sömu tímaflækjur: $\mathcal{O}(n \log \log n)$ tíma að forreikna og $\text{isp}(\dots)$ fyrirspurnin tekur $\mathcal{O}(1)$ tíma.
- ▶ Nýja $\text{factor}(\dots)$ fyrirspurnin tekur $\mathcal{O}(\quad)$ tíma því hún þarf að heimsækja hvern frumþátt tölunnar.

- ▶ Þessi útgáfa er ekki verri en hin á neinn veg, og því er sniðugt að nota hana alltaf.
- ▶ Hún hefur sömu tímaflækjur: $\mathcal{O}(n \log \log n)$ tíma að forreikna og $\text{isp}(\dots)$ fyrirspurnin tekur $\mathcal{O}(1)$ tíma.
- ▶ Nýja $\text{factor}(\dots)$ fyrirspurnin tekur $\mathcal{O}(\log n)$ tíma því hún þarf að heimsækja hvern frumþátt tölunnar.

- ▶ Reiknirit Pollards er reiknirit sem byggir á rásaleit til að finna þátt í samsettri tölu.

- ▶ Reiknirit Pollards er reiknirit sem byggir á rásaleit til að finna þátt í samsettri tölu.
- ▶ Reikniritið ákvarðar hvort talan n sé samsett í $\mathcal{O}(\sqrt{a})$ tíma, þar sem a er minnsti frumþáttur n .

- ▶ Reiknirit Pollards er reiknirit sem byggir á rásaleit til að finna þátt í samsettri tölu.
- ▶ Reikniritið ákvarðar hvort talan n sé samsett í $\mathcal{O}(\sqrt{a})$ tíma, þar sem a er minnsti frumþáttur n .
- ▶ Reikniritið finnur þátt í samsettri tölu n í $\mathcal{O}(\sqrt{a})$ tíma, þar sem a er minnsti frumþáttur n .

- ▶ Reiknirit Pollards er reiknirit sem byggir á rásaleit til að finna þátt í samsettri tölu.
- ▶ Reikniritið ákvarðar hvort talan n sé samsett í $\mathcal{O}(\sqrt{a})$ tíma, þar sem a er minnsti frumþáttur n .
- ▶ Reikniritið finnur þátt í samsettri tölu n í $\mathcal{O}(\sqrt{a})$ tíma, þar sem a er minnsti frumþáttur n .
- ▶ Nú gildir að $a \leq \sqrt{n}$ og því tekur reikniritið $\mathcal{O}(\sqrt[4]{n})$ tíma.

- ▶ Reiknirit Pollards er reiknirit sem byggir á rásaleit til að finna þátt í samsettri tölu.
- ▶ Reikniritið ákvarðar hvort talan n sé samsett í $\mathcal{O}(\sqrt{a})$ tíma, þar sem a er minnsti frumþáttur n .
- ▶ Reikniritið finnur þátt í samsettri tölu n í $\mathcal{O}(\sqrt{a})$ tíma, þar sem a er minnsti frumþáttur n .
- ▶ Nú gildir að $a \leq \sqrt{n}$ og því tekur reikniritið $\mathcal{O}(\sqrt[4]{n})$ tíma.
- ▶ Þetta er því töluverð bæting.

- ▶ Reiknirit Pollards er reiknirit sem byggir á rásaleit til að finna þátt í samsettri tölu.
- ▶ Reikniritið ákvarðar hvort talan n sé samsett í $\mathcal{O}(\sqrt{a})$ tíma, þar sem a er minnsti frumþáttur n .
- ▶ Reikniritið finnur þátt í samsettri tölu n í $\mathcal{O}(\sqrt{a})$ tíma, þar sem a er minnsti frumþáttur n .
- ▶ Nú gildir að $a \leq \sqrt{n}$ og því tekur reikniritið $\mathcal{O}(\sqrt[4]{n})$ tíma.
- ▶ Þetta er því töluverð bæting.
- ▶ Við þurfum samt fyrst úr skugga um að n sé framtala.

- ▶ Reiknirit Pollards er reiknirit sem byggir á rásaleit til að finna þátt í samsettri tölu.
- ▶ Reikniritið ákvarðar hvort talan n sé samsett í $\mathcal{O}(\sqrt{a})$ tíma, þar sem a er minnsti frumþáttur n .
- ▶ Reikniritið finnur þátt í samsettri tölu n í $\mathcal{O}(\sqrt{a})$ tíma, þar sem a er minnsti frumþáttur n .
- ▶ Nú gildir að $a \leq \sqrt{n}$ og því tekur reikniritið $\mathcal{O}(\sqrt[4]{n})$ tíma.
- ▶ Þetta er því töluverð bæting.
- ▶ Við þurfum samt fyrst úr skugga um að n sé framtala.
- ▶ Við megum þó ekki nota tæmandi leit til þess því þá bætist tímaflækjan ekkert.

- ▶ Reiknirit Pollards er reiknirit sem byggir á rásaleit til að finna þátt í samsettri tölu.
- ▶ Reikniritið ákvarðar hvort talan n sé samsett í $\mathcal{O}(\sqrt{a})$ tíma, þar sem a er minnsti frumþáttur n .
- ▶ Reikniritið finnur þátt í samsettri tölu n í $\mathcal{O}(\sqrt{a})$ tíma, þar sem a er minnsti frumþáttur n .
- ▶ Nú gildir að $a \leq \sqrt{n}$ og því tekur reikniritið $\mathcal{O}(\sqrt[4]{n})$ tíma.
- ▶ Þetta er því töluverð bæting.
- ▶ Við þurfum samt fyrst úr skugga um að n sé framtala.
- ▶ Við megum þó ekki nota tæmandi leit til þess því þá bætist tímaflækjan ekkert.
- ▶ Líkt og með reiknirit Millers og Rabins þá mun ég ekki fara í smáatriði hér.

```

49 ll rho(ll n)
50 { // skilar vonandi thaetti i |n|
51   ll s[8] = {2, 3, 4, 5, 7, 11, 13, 1031}, i, j, a, x, y, d;
52   for (a = 1;; a++) rep(j, 8)
53   {
54     x = y = s[j], d = 1;
55     while (d == 1)
56     {
57       x = (bigprod(x, x, n) + a)%n;
58       y = (bigprod(y, y, n) + a)%n;
59       y = (bigprod(y, y, n) + a)%n;
60       d = gcd(llabs(x - y), n);
61     }
62     if (d != n) return d;
63   }
64 }

```

```

78 void pollard_rho(ll n)
79 { // notar rho(...) ad ofan til ad thatta |n| og setur thaettina i |a|
80   c = 0;
81   ll i, s[200], ss = 0, p[6] = {2, 3, 5, 7, 11, 13};
82   rep(i, 6) while (n%p[i] == 0) n /= p[i], a[++c] = p[i];
83   s[ss++] = n;
84   if (n == 1) return;
85   while (ss > 0)
86   {
87     ll k = s[--ss];
88     if (miller_rabin(k)) a[++c] = k;
89     else
90     {
91       ll r = rho(k);
92       s[ss++] = r;
93       s[ss++] = k/r;
94     }
95   }
96 }

```

- ▶ Eftirfarandi jöfnur eru merkilegar hagnýtingar á frumþáttun.

- ▶ Eftirfarandi jöfnur eru merkilegar hagnýtingar á frumbáttun.
- ▶ Látum $n = p_1^{e_1} \cdot \dots \cdot p_m^{e_m}$, þar sem p_1, \dots, p_m eru frumtölur og e_1, \dots, e_m eru heiltölur stærri en 1.

- ▶ Eftirfarandi jöfnur eru merkilegar hagnýtingar á frumbáttun.
- ▶ Látum $n = p_1^{e_1} \cdot \dots \cdot p_m^{e_m}$, þar sem p_1, \dots, p_m eru frumtölur og e_1, \dots, e_m eru heiltölur stærri en 1.
- ▶ Við fáum þá eftirfarandi föll:

- ▶ Eftirfarandi jöfnur eru merkilegar hagnýtingar á frumbáttun.
- ▶ Látum $n = p_1^{e_1} \cdot \dots \cdot p_m^{e_m}$, þar sem p_1, \dots, p_m eru frumtölur og e_1, \dots, e_m eru heiltölur stærri en 1.
- ▶ Við fáum þá eftirfarandi föll:
 - ▶ Fjöldi deila n :

$$d(n) = \prod_{k=1}^r (e_k + 1).$$

- ▶ Eftirfarandi jöfnur eru merkilegar hagnýtingar á frumbáttun.
- ▶ Látum $n = p_1^{e_1} \cdot \dots \cdot p_m^{e_m}$, þar sem p_1, \dots, p_m eru frumtölur og e_1, \dots, e_m eru heiltölur stærri en 1.
- ▶ Við fáum þá eftirfarandi föll:
 - ▶ Fjöldi deila n :

$$d(n) = \prod_{k=1}^r (e_k + 1).$$

- ▶ Summa deila n :

$$\sigma(n) = \prod_{k=1}^r \frac{p_i^{e_i+1} - 1}{p_i - 1}.$$

- ▶ Eftirfarandi jöfnur eru merkilegar hagnýtingar á frumbáttun.
- ▶ Látum $n = p_1^{e_1} \cdot \dots \cdot p_m^{e_m}$, þar sem p_1, \dots, p_m eru frumtölur og e_1, \dots, e_m eru heiltölur stærri en 1.
- ▶ Við fáum þá eftirfarandi föll:
 - ▶ Fjöldi deila n :

$$d(n) = \prod_{k=1}^r (e_k + 1).$$

- ▶ Summa deila n :

$$\sigma(n) = \prod_{k=1}^r \frac{p_i^{e_i+1} - 1}{p_i - 1}.$$

- ▶ Fjöldi jákvæðra heiltana k , þannig að $\gcd(n, k) = 1$:

$$\phi(n) = n \prod_{k=1}^r (1 - 1/p_i).$$

- ▶ Eftirfarandi jöfnur eru merkilegar hagnýtingar á frumþáttun.
- ▶ Látum $n = p_1^{e_1} \cdot \dots \cdot p_m^{e_m}$, þar sem p_1, \dots, p_m eru frumtölur og e_1, \dots, e_m eru heiltölur stærri en 1.
- ▶ Við fáum þá eftirfarandi föll:
 - ▶ Fjöldi deila n :

$$d(n) = \prod_{k=1}^r (e_k + 1).$$

- ▶ Summa deila n :

$$\sigma(n) = \prod_{k=1}^r \frac{p_i^{e_i+1} - 1}{p_i - 1}.$$

- ▶ Fjöldi jákvæðra heiltana k , þannig að $\gcd(n, k) = 1$:

$$\phi(n) = n \prod_{k=1}^r (1 - 1/p_i).$$

- ▶ Einnig gefur setning kennd við Euler afhæfingu á litlu setningu Fermats:

$$a^{\phi(m)} = 1 \pmod{m}.$$

ef $\gcd(a, n) = 1$.

