

Talnafræði

Stærsti samdeilir og minnsta samfeldi

Bergur Snorrason

17. mars 2021

- ▶ Látum a , b , g og h vera jákvæðar heiltölur.

- ▶ Látum a , b , g og h vera jákvæðar heiltölur.
- ▶ Við segjum að talan g sé *samdeilir* a og b ef g deilir bæði a og b .

- ▶ Látum a , b , g og h vera jákvæðar heiltölur.
- ▶ Við segjum að talan g sé *samdeilir* a og b ef g deilir bæði a og b .
- ▶ Til dæmis ef $a = 2$ og $b = 4$ þá gæti g verið annað hvort 1 eða 2.

- ▶ Látum a , b , g og h vera jákvæðar heiltölur.
- ▶ Við segjum að talan g sé *samdeilir* a og b ef g deilir bæði a og b .
- ▶ Til dæmis ef $a = 2$ og $b = 4$ þá gæti g verið annað hvort 1 eða 2.
- ▶ Við segjum að talan h sé *samfeldi* a og b ef bæði a og b deila h .

- ▶ Látum a , b , g og h vera jákvæðar heiltölur.
- ▶ Við segjum að talan g sé *samdeilir* a og b ef g deilir bæði a og b .
- ▶ Til dæmis ef $a = 2$ og $b = 4$ þá gæti g verið annað hvort 1 eða 2.
- ▶ Við segjum að talan h sé *samfeldi* a og b ef bæði a og b deila h .
- ▶ Til dæmis ef $a = 2$ og $b = 4$ þá gæti h verið 4, 8 eða margar aðrar tölur.

- ▶ Látum a , b , g og h vera jákvæðar heiltölur.
- ▶ Við segjum að talan g sé *samdeilir* a og b ef g deilir bæði a og b .
- ▶ Til dæmis ef $a = 2$ og $b = 4$ þá gæti g verið annað hvort 1 eða 2.
- ▶ Við segjum að talan h sé *samfeldi* a og b ef bæði a og b deila h .
- ▶ Til dæmis ef $a = 2$ og $b = 4$ þá gæti h verið 4, 8 eða margar aðrar tölur.
- ▶ *Stærsta samdeili* a og b táknum við með $\gcd(a, b)$.

- ▶ Látum a , b , g og h vera jákvæðar heiltölur.
- ▶ Við segjum að talan g sé *samdeilir* a og b ef g deilir bæði a og b .
- ▶ Til dæmis ef $a = 2$ og $b = 4$ þá gæti g verið annað hvort 1 eða 2.
- ▶ Við segjum að talan h sé *samfeldi* a og b ef bæði a og b deila h .
- ▶ Til dæmis ef $a = 2$ og $b = 4$ þá gæti h verið 4, 8 eða margar aðrar tölur.
- ▶ *Stærsta samdeili* a og b táknum við með $\gcd(a, b)$.
- ▶ *Minnsta samfeldi* a og b táknum við með $\text{lcm}(a, b)$.

- ▶ Látum a , b , g og h vera jákvæðar heiltölur.
- ▶ Við segjum að talan g sé *samdeilir* a og b ef g deilir bæði a og b .
- ▶ Til dæmis ef $a = 2$ og $b = 4$ þá gæti g verið annað hvort 1 eða 2.
- ▶ Við segjum að talan h sé *samfeldi* a og b ef bæði a og b deila h .
- ▶ Til dæmis ef $a = 2$ og $b = 4$ þá gæti h verið 4, 8 eða margar aðrar tölur.
- ▶ *Stærsta samdeili* a og b táknum við með $\gcd(a, b)$.
- ▶ *Minnsta samfeldi* a og b táknum við með $\text{lcm}(a, b)$.
- ▶ Við munum einblína á að reikna stærsta samdeili því $\text{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b$.

- ▶ Hvernig finnum við stærsta samdeili tveggja talna?

- ▶ Hvernig finnum við stærsta samdeili tveggja talna?
- ▶ Látum a og b vera jákvæðar heiltölur og g vera stærsta samdeilir þeirra.

- ▶ Hvernig finnum við stærsta samdeili tveggja talna?
- ▶ Látum a og b vera jákvæðar heiltölur og g vera stærsta samdeilir þeirra.
- ▶ Gerum einnig ráð fyrir að $a < b$ (ef $a = b$ þá er $g = a$).

- ▶ Hvernig finnum við stærsta samdeili tveggja talna?
- ▶ Látum a og b vera jákvæðar heiltölur og g vera stærsta samdeilir þeirra.
- ▶ Gerum einnig ráð fyrir að $a < b$ (ef $a = b$ þá er $g = a$).
- ▶ Tökum eftir að g deilir líka $b - a$.

- ▶ Hvernig finnum við stærsta samdeili tveggja talna?
- ▶ Látum a og b vera jákvæðar heiltölur og g vera stærsta samdeilir þeirra.
- ▶ Gerum einnig ráð fyrir að $a < b$ (ef $a = b$ þá er $g = a$).
- ▶ Tökum eftir að g deilir líka $b - a$.
- ▶ Svo okkur nægir að finna stærsta samdeili a og $b - a$.

- ▶ Hvernig finnum við stærsta samdeili tveggja talna?
- ▶ Látum a og b vera jákvæðar heiltölur og g vera stærsta samdeilir þeirra.
- ▶ Gerum einnig ráð fyrir að $a < b$ (ef $a = b$ þá er $g = a$).
- ▶ Tökum eftir að g deilir líka $b - a$.
- ▶ Svo okkur nægir að finna stærsta samdeili a og $b - a$.

```
12 ll slow_gcd(ll a, ll b)
13 {
14     if (a == b) return a;
15     if (a > b) return gcd(b, a);
16     return gcd(a, b - a);
17 }
```

- Tökum eftir að ef $a = 2$ hefur þetta fall tímaflækjuna $\mathcal{O}(\quad)$.

- ▶ Tökum eftir að ef $a = 2$ hefur þetta fall tímaflækjuna $\mathcal{O}(b)$.

- ▶ Tökum eftir að ef $a = 2$ hefur þetta fall tímaflækjuna $\mathcal{O}(b)$.
- ▶ Svo þetta verður almennt aldrei betra en $\mathcal{O}(\quad)$.

- ▶ Tökum eftir að ef $a = 2$ hefur þetta fall tímaflækjuna $\mathcal{O}(b)$.
- ▶ Svo þetta verður almennt aldrei betra en $\mathcal{O}(\max(a, b))$.

- ▶ Tökum eftir að ef $a = 2$ hefur þetta fall tímaflækjuna $\mathcal{O}(b)$.
- ▶ Svo þetta verður almennt aldrei betra en $\mathcal{O}(\max(a, b))$.
- ▶ En við getum bætt þetta.

- ▶ Tökum eftir að ef $a = 2$ hefur þetta fall tímaflækjuna $\mathcal{O}(b)$.
- ▶ Svo þetta verður almennt aldrei betra en $\mathcal{O}(\max(a, b))$.
- ▶ En við getum bætt þetta.
- ▶ Skoðum eitt einfalt dæmi.

26 101
-> 26 75

26 101

-> 26 75

-> 26 49

26 101

-> 26 75

-> 26 49

-> 26 23

26 101

-> 26 75

-> 26 49

-> 26 23

-> 23 26

26 101
-> 26 75
-> 26 49
-> 26 23
-> 23 26
-> 23 3

26 101
-> 26 75
-> 26 49
-> 26 23
-> 23 26
-> 23 3
-> 3 23

26 101
-> 26 75
-> 26 49
-> 26 23
-> 23 26
-> 23 3
-> 3 23
-> 3 20

26 101
-> 26 75
-> 26 49
-> 26 23
-> 23 26
-> 23 3
-> 3 23
-> 3 20
-> 3 17

26 101
-> 26 75
-> 26 49
-> 26 23
-> 23 26
-> 23 3
-> 3 23
-> 3 20
-> 3 17
-> 3 14

26 101
-> 26 75
-> 26 49
-> 26 23
-> 23 26
-> 23 3
-> 3 23
-> 3 20
-> 3 17
-> 3 14
-> 3 11

26 101
-> 26 75
-> 26 49
-> 26 23
-> 23 26
-> 23 3
-> 3 23
-> 3 20
-> 3 17
-> 3 14
-> 3 11
-> 3 8

26 101
-> 26 75
-> 26 49
-> 26 23
-> 23 26
-> 23 3
-> 3 23
-> 3 20
-> 3 17
-> 3 14
-> 3 11
-> 3 8
-> 3 5

26 101
-> 26 75
-> 26 49
-> 26 23
-> 23 26
-> 23 3
-> 3 23
-> 3 20
-> 3 17
-> 3 14
-> 3 11
-> 3 8
-> 3 5
-> 3 2

26 101
-> 26 75
-> 26 49
-> 26 23
-> 23 26
-> 23 3
-> 3 23
-> 3 20
-> 3 17
-> 3 14
-> 3 11
-> 3 8
-> 3 5
-> 3 2
-> 2 3

26 101
-> 26 75
-> 26 49
-> 26 23
-> 23 26
-> 23 3
-> 3 23
-> 3 20
-> 3 17
-> 3 14
-> 3 11
-> 3 8
-> 3 5
-> 3 2
-> 2 3
-> 2 1

26 101
-> 26 75
-> 26 49
-> 26 23
-> 23 26
-> 23 3
-> 3 23
-> 3 20
-> 3 17
-> 3 14
-> 3 11
-> 3 8
-> 3 5
-> 3 2
-> 2 3
-> 2 1
-> 1 2

	26	101
->	26	75
->	26	49
->	26	23
->	23	26
->	23	3
->	3	23
->	3	20
->	3	17
->	3	14
->	3	11
->	3	8
->	3	5
->	3	2
->	2	3
->	2	1
->	1	2
->	1	1

- ▶ Við getum tekið saman þau skref sem eiga sér stað þangað til $a > b$.

- ▶ Við getum tekið saman þau skref sem eiga sér stað þangað til $a > b$.
- ▶ Við finnum q þannig að $b - a \cdot q$ sé jákvætt og minna en a .

- ▶ Við getum tekið saman þau skref sem eiga sér stað þangað til $a > b$.
- ▶ Við finnum q þannig að $b - a \cdot q$ sé jákvætt og minna en a .

- ▶ Við getum tekið saman þau skref sem eiga sér stað þangað til $a > b$.
- ▶ Við finnum q þannig að $b - a \cdot q$ sé jákvætt og minna en a .
- ▶ En við getum fundið þessa tölu með leifareikningi.

- ▶ Við getum tekið saman þau skref sem eiga sér stað þangað til $a > b$.
- ▶ Við finnum q þannig að $b - a \cdot q$ sé jákvætt og minna en a .
- ▶ En við getum fundið þessa tölu með leifareikningi.
- ▶ Við notum því $\gcd(a, b) = \gcd(r, a)$ í staðinn fyrir $\gcd(a, b) = \gcd(a, b - a)$, þar sem r er leif b með tilliti til a .

26 101

26 101
-> 23 26

26 101
-> 23 26
-> 3 23

26 101
-> 23 26
-> 3 23
-> 2 3

26 101
-> 23 26
-> 3 23
-> 2 3
-> 1 2

	26	101
->	23	26
->	3	23
->	2	3
->	1	2
->	0	1

- ▶ Útfærslan einfaldast töluvert með þessari bætingu.

- Útfærslan einfaldast töluvert með þessari bætingu.

```
7 ll gcd(ll a, ll b)
8 {
9     return b == 0 ? a : gcd(b, a%b);
10 }
```

- Útfærslan einfaldast töluvert með þessari bætingu.

```
7 int gcd(int a, int b)
8 {
9     return b == 0 ? a : gcd(b, a%b);
10 }
```

- Þessi útfærsla verður $\mathcal{O}(\quad)$.

- Útfærslan einfaldast töluvert með þessari bætingu.

```
7 int gcd(int a, int b)
8 {
9     return b == 0 ? a : gcd(b, a%b);
10 }
```

- Þessi útfærsla verður $\mathcal{O}(\log \max(a, b))$.

- Útfærslan einfaldast töluvert með þessari bætingu.

```
7  ll gcd(ll a, ll b)
8  {
9      return b == 0 ? a : gcd(b, a%b);
10 }
```

- Þessi útfærsla verður $\mathcal{O}(\log \max(a, b))$.
- Ástæðan fyrir þessari bætingu er að ef a minnkar lítið eftir eitt skref þá verður lítill munur á a og b , svo næst minnkar a meira.

- Útfærslan einfaldast töluvert með þessari bætingu.

```
7 int gcd(int a, int b)
8 {
9     return b == 0 ? a : gcd(b, a%b);
10 }
```

- Þessi útfærsla verður $\mathcal{O}(\log \max(a, b))$.
- Ástæðan fyrir þessari bætingu er að ef a minnkar lítið eftir eitt skref þá verður lítill munur á a og b , svo næst minnkar a meira.
- Við kennum þetta reiknirit við Evklíð.

- Útfærslan einfaldast töluvert með þessari bætingu.

```
7 int gcd(int a, int b)
8 {
9     return b == 0 ? a : gcd(b, a%b);
10 }
```

- Þessi útfærsla verður $\mathcal{O}(\log \max(a, b))$.
- Ástæðan fyrir þessari bætingu er að ef a minnkar lítið eftir eitt skref þá verður lítill munur á a og b , svo næst minnkar a meira.
- Við kennum þetta reiknirit við Evklíð.
- Þetta ferli er einnig kallað *keðjudeiling*.

Jafna Bézouts

- ▶ Algengt er að nota keðjudeilingu til að leysa jöfnu Bézouts.

Jafna Bézouts

- ▶ Algengt er að nota keðjudeilingu til að leysa jöfnu Bézouts.
- ▶ Látum a og b vera jákvæðar heiltölur.

Jafna Bézouts

- ▶ Algengt er að nota keðjudeilingu til að leysa jöfnu Bézouts.
- ▶ Látum a og b vera jákvæðar heiltölur.
- ▶ Þá eru til heiltölur x og y þannig að $a \cdot x + b \cdot y = \gcd(a, b)$.

Jafna Bézouts

- ▶ Algengt er að nota keðjudeilingu til að leysa jöfnu Bézouts.
- ▶ Látum a og b vera jákvæðar heiltölur.
- ▶ Þá eru til heiltölur x og y þannig að $a \cdot x + b \cdot y = \gcd(a, b)$.
- ▶ Þessi jafna kallast *jafna Bézouts*.

Jafna Bézouts

- ▶ Algengt er að nota keðjudeilingu til að leysa jöfnu Bézouts.
- ▶ Látum a og b vera jákvæðar heiltölur.
- ▶ Þá eru til heiltölur x og y þannig að $a \cdot x + b \cdot y = \gcd(a, b)$.
- ▶ Þessi jafna kallast *jafna Bézouts*.
- ▶ Við notum svo kallaða *útvíkkaða keðjudeilingu* til að finna tölurnar x og y .

Jafna Bézouts

- ▶ Algengt er að nota keðjudeilingu til að leysa jöfnu Bézouts.
- ▶ Látum a og b vera jákvæðar heiltölur.
- ▶ Þá eru til heiltölur x og y þannig að $a \cdot x + b \cdot y = \gcd(a, b)$.
- ▶ Þessi jafna kallast *jafna Bézouts*.
- ▶ Við notum svo kallaða *útvíkkaða keðjudeilingu* til að finna tölurnar x og y .

```
7 void swap(ll* x, ll* y) { ll s = *x; *x = *y; *y = s; }
8 ll egcd(ll a, ll b, ll* x, ll* y)
9 {
10     if (b == 0)
11     {
12         *x = 1, *y = 0;
13         return a;
14     }
15     ll r = egcd(b, a%b, x, y);
16     *x -= a/b>(*y);
17     swap(x, y);
18     return r;
19 }
```

- ▶ Algengasta hagnýting jöfn Bézouts er til að finna margföldunarandhverfur.

- ▶ Algengasta hagnýting jöfn Bézouts er til að finna margföldunarandhverfur.
- ▶ Við höfum áður gert það með litlu setningu Fermats.

- ▶ Algengasta hagnýting jöfn Bézouts er til að finna margföldunarandhverfur.
- ▶ Við höfum áður gert það með litlu setningu Fermats.
- ▶ Gerum ráð fyrir að a og m séu jákvæðar heiltölur þannig að $\gcd(a, m) = 1$.

- ▶ Algengasta hagnýting jöfn Bézouts er til að finna margföldunarandhverfur.
- ▶ Við höfum áður gert það með litlu setningu Fermats.
- ▶ Gerum ráð fyrir að a og m séu jákvæðar heiltölur þannig að $\gcd(a, m) = 1$.
- ▶ Látum svo heiltölurnar x og y leysa Bézout jöfnuna $a \cdot x + m \cdot y = 1$.

- ▶ Algengasta hagnýting jöfn Bézouts er til að finna margföldunarandhverfur.
- ▶ Við höfum áður gert það með litlu setningu Fermats.
- ▶ Gerum ráð fyrir að a og m séu jákvæðar heiltölur þannig að $\gcd(a, m) = 1$.
- ▶ Látum svo heiltölurnar x og y leysa Bézout jöfnuna $a \cdot x + m \cdot y = 1$.
- ▶ Þá fæst að x er margföldunarandhverfa a með tilliti til m .

- ▶ Algengasta hagnýting jöfn Bézouts er til að finna margföldunarandhverfur.
- ▶ Við höfum áður gert það með litlu setningu Fermats.
- ▶ Gerum ráð fyrir að a og m séu jákvæðar heiltölur þannig að $\gcd(a, m) = 1$.
- ▶ Látum svo heiltölurnar x og y leysa Bézout jöfnuna $a \cdot x + m \cdot y = 1$.
- ▶ Þá fæst að x er margföldunarandhverfa a með tilliti til m .
- ▶ Ef $\gcd(a, m) \neq 1$ þá er margföldunarandhverfa a ekki til.

- ▶ Algengasta hagnýting jöfn Bézouts er til að finna margföldunarandhverfur.
- ▶ Við höfum áður gert það með litlu setningu Fermats.
- ▶ Gerum ráð fyrir að a og m séu jákvæðar heiltölur þannig að $\gcd(a, m) = 1$.
- ▶ Látum svo heiltölurnar x og y leysa Bézout jöfnuna $a \cdot x + m \cdot y = 1$.
- ▶ Þá fæst að x er margföldunarandhverfa a með tilliti til m .
- ▶ Ef $\gcd(a, m) \neq 1$ þá er margföldunarandhverfa a ekki til.

```
19 ll mulinv(ll a, ll m)
20 {
21     ll x, y, g;
22     g = egcd(a, m, &x, &y);
23     assert(g == 1);
24     return x;
25 }
```

- ▶ Algengasta hagnýting jöfn Bézouts er til að finna margföldunarandhverfur.
- ▶ Við höfum áður gert það með litlu setningu Fermats.
- ▶ Gerum ráð fyrir að a og m séu jákvæðar heiltölur þannig að $\gcd(a, m) = 1$.
- ▶ Látum svo heiltölurnar x og y leysa Bézout jöfnuna $a \cdot x + m \cdot y = 1$.
- ▶ Þá fæst að x er margföldunarandhverfa a með tilliti til m .
- ▶ Ef $\gcd(a, m) \neq 1$ þá er margföldunarandhverfa a ekki til.

```

19 ll mulinv(ll a, ll m)
20 {
21     ll x, y, g;
22     g = egcd(a, m, &x, &y);
23     assert(g == 1);
24     return x;
25 }

```

- ▶ Takið eftir að x getur verið neikvæð.

- ▶ Algengasta hagnýting jöfn Bézouts er til að finna margföldunarandhverfur.
- ▶ Við höfum áður gert það með litlu setningu Fermats.
- ▶ Gerum ráð fyrir að a og m séu jákvæðar heiltölur þannig að $\gcd(a, m) = 1$.
- ▶ Látum svo heiltölurnar x og y leysa Bézout jöfnuna $a \cdot x + m \cdot y = 1$.
- ▶ Þá fæst að x er margföldunarandhverfa a með tilliti til m .
- ▶ Ef $\gcd(a, m) \neq 1$ þá er margföldunarandhverfa a ekki til.

```

19 ll mulinv(ll a, ll m)
20 {
21     ll x, y, g;
22     g = egcd(a, m, &x, &y);
23     assert(g == 1);
24     return x;
25 }

```

- ▶ Takið eftir að x getur verið neikvæð.
- ▶ Til að koma í veg fyrir það má breyta skilagildinu í $(x \% m + m) \% m$.

- ▶ Takið eftir að þetta reiknirit virkar stundum þegar m er ekki frumtala en litla setning Fermats virkar bara þegar m er frumtala.

