Talnafræði

Leifareikningur

Bergur Snorrason

10. mars 2021

Leifareikningur

- Látum a og m vera jákvæðar heiltölur.

Leifareikningur

- Látum a og m vera jákvæðar heiltölur.
- Alltaf eru til jákvæðar heiltölur $r < m$ og q þannig $a = q \cdot m + r$.

Leifareikningur

- Látum a og m vera jákvæðar heiltölur.
- Alltaf eru til jákvæðar heiltölur $r < m$ og q þannig $a = q \cdot m + r$.
- Við segjum þá að r sé *leif a með tilliti til m*.

Leifareikningur

- Látum a og m vera jákvæðar heiltölur.
- Alltaf eru til jákvæðar heiltölur $r < m$ og q þannig $a = q \cdot m + r$.
- Við segjum þá að r sé *leif* a *með tilliti til* m.
- Við skrifum svo $b = a \mod m$ ef a og b hafa sömu leif með tilliti til m.

Leifareikningur

- Látum a og m vera jákvæðar heiltölur.
- Alltaf eru til jákvæðar heiltölur $r < m$ og q þannig $a = q \cdot m + r$.
- Við segjum þá að r sé *leif* a *með tilliti til* m.
- Við skrifum svo $b = a \mod m$ ef a og b hafa sömu leif með tilliti til m.
- Flest forritunarmál reikna þessa leif með `a%m`.

Leifareikningur

- Látum a og m vera jákvæðar heiltölur.
- Alltaf eru til jákvæðar heiltölur $r < m$ og q þannig $a = q \cdot m + r$.
- Við segjum þá að r sé *leif a með tilliti til m*.
- Við skrifum svo $b = a \mod m$ ef a og b hafa sömu leif með tilliti til m.
- Flest forritunarmál reikna þessa leif með `a%m`.
- Gerum nú ráð fyrir að við séum með jákvæðar heiltölur a_1, a_2, m, og $r_1 = a_1 \mod m$ og $r_2 = a_2 \mod m$.

Leifareikningur

- Látum a og m vera jákvæðar heiltölur.
- Alltaf eru til jákvæðar heiltölur $r < m$ og q þannig $a = q \cdot m + r$.
- Við segjum þá að r sé *leif a með tilliti til m*.
- Við skrifum svo $b = a \mod m$ ef a og b hafa sömu leif með tilliti til m.
- Flest forritunarmál reikna þessa leif með `a%m`.
- Gerum nú ráð fyrir að við séum með jákvæðar heiltölur a_1, a_2, m, og $r_1 = a_1 \mod m$ og $r_2 = a_2 \mod m$.
- Þá gildir að

$$r_1 + r_2 = a_1 + a_2 \mod m$$

og

$$r_1 \cdot r_2 = a_1 \cdot a_2 \mod m.$$

- Þið þurfið að passa ykkur ef þið eruð með neikvæðar tölur.

- Þið þurfið að passa ykkur ef þið eruð með neikvæðar tölur.
- Til dæmis er ekki skilgreint hverju `(-10)%3` skilar í `C`.

- Þið þurfið að passa ykkur ef þið eruð með neikvæðar tölur.
- Til dæmis er ekki skilgreint hverju `(-10)%3` skilar í `C`.
- Við vitum ekki hvort það skili -1 eða 2.

- Þið þurfið að passa ykkur ef þið eruð með neikvæðar tölur.
- Til dæmis er ekki skilgreint hverju `(-10)%3` skilar í `C`.
- Við vitum ekki hvort það skili `-1` eða `2`.
- Til að komast í kringum þessa óvissu notum við frekar `(a%m + m)%m` ef `a` getur verið neikvæð.

- Þið þurfið að passa ykkur ef þið eruð með neikvæðar tölur.
- Til dæmis er ekki skilgreint hverju `(-10)%3` skilar í `C`.
- Við vitum ekki hvort það skili `-1` eða `2`.
- Til að komast í kringum þessa óvissu notum við frekar `(a%m + m)%m` ef `a` getur verið neikvæð.
- Þetta virkar því `a%m + m` verður alltaf jákvæð.

- Stundum þurfum við að geta deilt í leifareikningi.

- Stundum þurfum við að geta deilt í leifareikningi.
- Þetta er ekki hægt að gera með hefðbundinni deilingu.

- Stundum þurfum við að geta deilt í leifareikningi.
- Þetta er ekki hægt að gera með hefðbundinni deilingu.
- Við látum b^{-1} tákna þá tölu sem uppfyllir að $1 = b \cdot b^{-1} \mod m$.

- Stundum þurfum við að geta deilt í leifareikningi.
- Þetta er ekki hægt að gera með hefðbundinni deilingu.
- Við látum b^{-1} tákna þá tölu sem uppfyllir að $1 = b \cdot b^{-1} \mod m$.
- Þessi tala er ekki alltaf til.

- Stundum þurfum við að geta deilt í leifareikningi.
- Þetta er ekki hægt að gera með hefðbundinni deilingu.
- Við látum b^{-1} tákna þá tölu sem uppfyllir að $1 = b \cdot b^{-1} \mod m$.
- Þessi tala er ekki alltaf til.
- Hún er þó alltaf til ef m er frumtala.

- Stundum þurfum við að geta deilt í leifareikningi.
- Þetta er ekki hægt að gera með hefðbundinni deilingu.
- Við látum b^{-1} tákna þá tölu sem uppfyllir að $1 = b \cdot b^{-1} \mod m$.
- Þessi tala er ekki alltaf til.
- Hún er þó alltaf til ef m er frumtala.
- Við skrifum svo stundum a/b í stað ab^{-1}.

- Stundum þurfum við að geta deilt í leifareikningi.
- Þetta er ekki hægt að gera með hefðbundinni deilingu.
- Við látum b^{-1} tákna þá tölu sem uppfyllir að $1 = b \cdot b^{-1} \mod m$.
- Þessi tala er ekki alltaf til.
- Hún er þó alltaf til ef m er frumtala.
- Við skrifum svo stundum a/b í stað ab^{-1}.
- En hvernig finnum við þessa tölu?

- Látum p vera frumtölu.

- Látum p vera frumtölu.
- Litla setning Fermats segir okkur að $a^p = a \mod p$.

- Látum p vera frumtölu.
- Litla setning Fermats segir okkur að $a^p = a \mod p$.
- Ef við margföldum báðum megin með a^{-2} fæst að $a^{p-2} = a^{-1} \mod p$.

- Látum p vera frumtölu.
- Litla setning Fermats segir okkur að $a^p = a \mod p$.
- Ef við margföldum báðum megin með a^{-2} fæst að $a^{p-2} = a^{-1} \mod p$.
- Svo eina sem við þurfum að gera er að reikna $a^{p-2} \mod p$.

- Látum p vera frumtölu.
- Litla setning Fermats segir okkur að $a^p = a \mod p$.
- Ef við margföldum báðum megin með a^{-2} fæst að $a^{p-2} = a^{-1} \mod p$.
- Svo eina sem við þurfum að gera er að reikna $a^{p-2} \mod p$.
- Gerum ráð fyrir að við séum með fall `modpow(x, n, m)` sem reiknar $x^n \mod m$ (við útfærum það á eftir).

- Látum p vera frumtölu.
- Litla setning Fermats segir okkur að $a^p = a \mod p$.
- Ef við margföldum báðum megin með a^{-2} fæst að $a^{p-2} = a^{-1} \mod p$.
- Svo eina sem við þurfum að gera er að reikna $a^{p-2} \mod p$.
- Gerum ráð fyrir að við séum með fall `modpow(x, n, m)` sem reiknar $x^n \mod m$ (við útfærum það á eftir).

```
ll mulinv(ll a, ll p)
{
    return modpow(a, p - 2, p);
}
```

- Látum p vera frumtölu.
- Litla setning Fermats segir okkur að $a^p = a \mod p$.
- Ef við margföldum báðum megin með a^{-2} fæst að $a^{p-2} = a^{-1} \mod p$.
- Svo eina sem við þurfum að gera er að reikna $a^{p-2} \mod p$.
- Gerum ráð fyrir að við séum með fall `modpow(x, n, m)` sem reiknar $x^n \mod m$ (við útfærum það á eftir).

```
ll mulinv(ll a, ll p)
{
    return modpow(a, p - 2, p);
}
```

- Tímaflækjan á þessari aðferð verður síðan sú sama og tímaflækjan á `modpow(...)`.

- Til að finna $a^{-1} \mod m$ ef m er ekki frumtala er ögn flóknara.

- Til að finna $a^{-1} \mod m$ ef m er ekki frumtala er ögn flóknara.
- Við skoðum það á eftir þegar við skoðum reiknirit Evklíðs.