Talnafræði

Stærsti samdeilir og minnsta samfeldi

Bergur Snorrason

March 11, 2024

- 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?
- 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 $b - a$.

```
ll slow_gcd(ll a, ll b)
{
    if (a == b) return a;
    if (a > b) return gcd(b, a);
    return gcd(a, b - a);
}
```

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

26 101

```
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 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.

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

- 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*.

- 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.

```
void swap(ll* x, ll* y) { ll s = *x; *x = *y; *y = s; }
ll egcd(ll a, ll b, ll* x, ll* y)
{
    if (b == 0)
    {
        *x = 1, *y = 0;
        return a;
    }
    ll r = egcd(b, a%b, x, y);
    *x -= a/b*(*y);
    swap(x, y);
    return r;
}
```

- Algeng 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.

```
ll mulinv(ll a, ll m)
{
    ll x, y, g;
    g = egcd(a, m, &x, &y);
    assert(g == 1);
    return x;
}
```

- 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.