Stærðfræðimynstur í tölvunarfræði

Vika 6

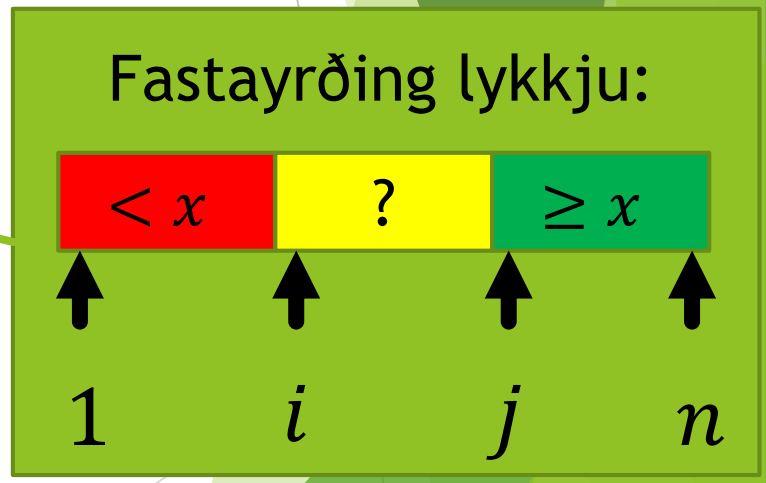
Kafli 3: Flækjustig helmingunarleitar og insertion sort

Kafli 4: Talnafræði, mátreikningur og dulritun

Helmingunarleit (binary search)

{
Notkun: i := leita(x, $a_1, a_2, \ldots, a_n$)
Fyrir: x er heiltala,
$a_1, a_2, \ldots, a_n$ eru heiltölur í vaxandi röð
Eftir: $1 \leq i \leq n+1$, $a_1, \ldots, a_{i-1} < x \leq a_i, \ldots, a_n$
}

stef leita(x : heiltala, $a_1, a_2, \ldots, a_n$: heiltölur)
    $i := 1$; $j := n + 1$
    meðan $i \neq j$
        { $1 \leq i \leq j \leq n+1$, $a_1, \ldots, a_{i-1} < x \leq a_j, \ldots, a_n$ }
        $m := \lfloor (i + j)/2 \rfloor$
        ef $a_m < x$ **þá** $i := m + 1$
        annars $j := m$
    skila i

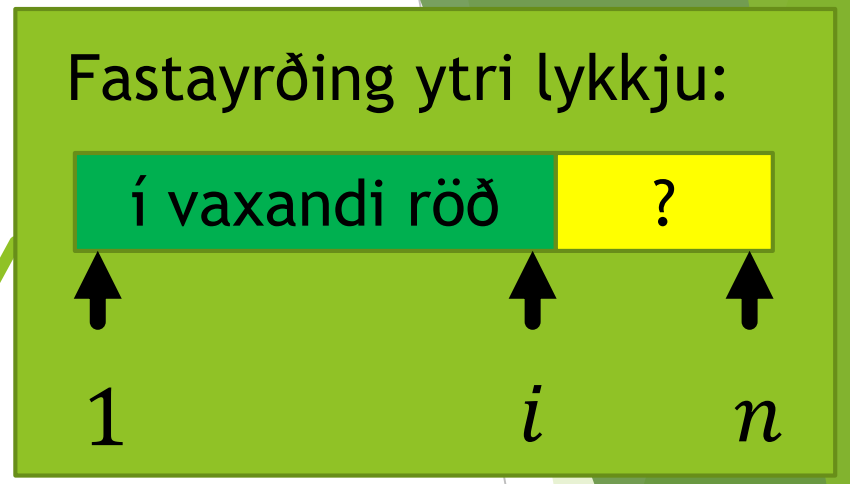


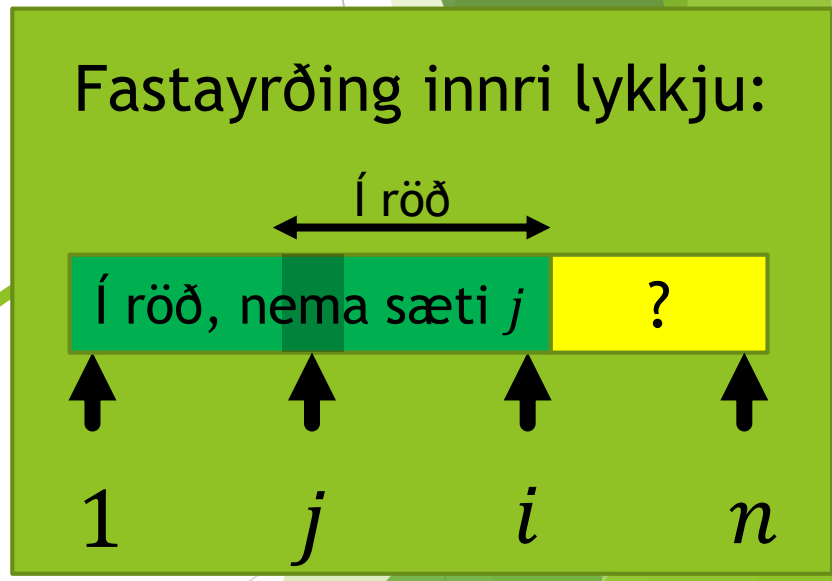
Hver er tímaflækja helmingunarleitar í versta tilfelli?

- **Lausn:** Teljum fjölda samanburða
  - Í hverri umferð lykkjunnar helmingast (a.m.k.) fjöldi óþekktra sæta, $\boldsymbol{j - i}$, sem í upphafi eru $\boldsymbol{n}$ talsins
    - Fjöldi umferða í lykkjunni er því í mesta lagi (fyrir $n > 0$)
      - $1 + log_2(n)$
  - Samanburðurinn $a_m < x$ er framkvæmdur einu sinni í hverri umferð lykkjunnar
    - Samtals $1 + log_2(n)$ sinnum í mesta lagi
  - Samanburðurinn $i \neq j$ er framkvæmdur einu sinni á undan hverri umferð lykkjunnar og einu sinni enn eftir að öllum umferðum er lokið
    - Samtals $2 + log_2(n)$ sinnum í mesta lagi
  - Heildarfjöldi samanburða er því $3 + 2\log_2(n)$
- Tímaflækja algrímsins er því $\Theta(\log(n))$, mun betri en línuleg leit

Röðun: Insertion sort

```
{
Notkun:     raða( a_1, a_2, …, a_n )
Fyrir:      a_1, a_2, …, a_n er runa af rauntölubreytum
Eftir:      Gildunum í rununni hefur verið umraðað
            svo gildin eru í vaxandi röð
}
stef raða( a_1, a_2, …, a_n: runa af rauntölubreytum )
    i := 0
    meðan i ≠ n
        { a_1, a_2, …, a_i er í vaxandi röð, 0 ≤ i ≤ n }
        i := i + 1;   j := i
        meðan j ≠ 1 og a_j < a_{j-1}
            { 1 ≤ j ≤ i ≤ n, a_j, a_{j+1}, …, a_i er í vaxandi röð,   }
            { a_1, a_2, …, a_{j-1}, a_{j+1}, …, a_i er einnig í vaxandi röð.   }
            { Gildið í sæti a_j er því ef til vill of aftarlega.   }
            m := a_j;   a_j := a_{j-1};   a_{j-1} := m;   j := j - 1
```





Víxlum gildunum í a_j og a_{j-1}
Færir gildið framar í rununni

Hver er tímaflækja insertion sort í versta tilfelli?

- **Lausn:** Teljum fjölda samanburða
  - Fjöldi umferða í ytri lykkjunni er $\boldsymbol{n}$, þar sem i hefur í byrjun hverrar umferðar gildin $i = 0,1, \dots, n-1$
    - Fyrir hverja slíka umferð ytri lykkjunnar verða í versta tilfelli farnar i umferðir innri lykkju, með i samanburðum $a_j < a_{j-1}$ auk $i+1$ samanburða $j \neq 1$
      - Heildarfjöldi: $[0 + 1 + \cdots + (n-1)] + [1 + 2 + \cdots + n] = n^2$
    - Í upphafi hverrar umferðar ytri lykkju og einnig eftir síðustu er framkvæmdur einn samanburður, samtals $n+1$ samanburður
  - Heildarfjöldi samanburða er því $\mathrm{n}^2 + n + 1$
- Tímaflækja algrímsins er því $\Theta(n^2)$

Talnafræði

- Deilanleiki (divisibility) og mátreikningur (modular arithmetic)
- Framsetning heiltalna (integer representation) og algrím
- Prímtölur (primes), stærstu samdeilar (greatest common divisor, GCD) og minnstu samfeldi (least common multiple, LCM, minnstu samnefnarar)
- Lausnir mátjafna (congruences)
- Gagnsemi mátjafna
- Dulritun (cryptography)

Deiling og deilanleiki

- **Skilgreining:** Ef a og b eru heiltölur, $a \neq 0$, þá segjum við að a **gangi upp í** b ef til er heiltala c þannig að $b = ac$
  - Þegar a gengur upp í b segjum við að a sé þáttur í b og að b sé margfeldi a
  - Ritháttur inn $a \mid b$ þýðir að a gengur upp í b
  - Ef $a \mid b$ þá er b/a heiltala
  - Ef a gengur ekki upp í b skrifum við $a \nmid b$
- Dæmi: $3 \mid 12$ en $5 \nmid 12$

Eiginleikar deilanleika

- **Setning:** Látum a, b og c vera heiltölur, $a \neq 0$
  1. Ef $a \mid b$ og $a \mid c$ þá $a \mid (b + c)$
  2. Ef $a \mid b$ þá $a \mid bc$ fyrir allar heiltölur c
  3. Ef $a \mid b$ og $b \mid c$ þá $a \mid c$
- **Sönnun á 1:** Þar eð $a \mid b$ er til heiltala n þannig að $b = na$. Þar eð $a \mid c$ er til heiltala m þannig að $c = ma$. Þá fæst $b + c = na + ma = (n + m)a$ og því er $b + c$ margfeldi a.
- **Fylgisetning (corollary):** Ef a, b og c eru heiltölur, $a \neq 0$, þannig að $a \mid b$ og $a \mid c$, þá $a \mid (mb + nc)$ fyrir allar heiltölur n og m

Deiling, kvóti og afgangur

- **Setning:** Ef a er heiltala og d er jákvæð heiltala þá er til ein og aðeins ein heiltala q og ein og aðeins ein heiltala r, þannig að $0 \leq r < d$ og $a = dq + r$
  - d er kallaður **deilirinn (divisor)**
  - a er kallaður **deilistofn (dividend)**
  - q er kallaður **kvótinn (quotient)**
  - r er kallaður **afgangurinn (remainder,** stundum **leif)**
- Dæmi:
  - Hver er kvótinn og afgangurinn þegar 101 er deilt með 11?
    - Svar: Kvótinn er $9 = 101\ div\ 11$, afgangurinn er $2 = 101\ mod\ 11$
  - Hver er kvótinn og afgangurinn þegar -11 er deilt með 3?
    - Svar: Kvótinn er $-4 = -11\ div\ 3$, afgangurinn er $1 = -11\ mod\ 3$

Föllin **div** og **mod**:

$$q = a\ \mathbf{div}\ d$$

$$r = a\ \mathbf{mod}\ d$$

Deilanleiki og mátreikningur

- **Skilgreining:** Ef a og b eru heiltölur og m er jákvæð heiltala þá er a **samleifa** b **mátað við** m þá og því aðeins að m gangi upp í $a - b$
  - Á ensku segjum við „a **is congruent to** b **modulo** m“
  - Ritháttur inn „$a \equiv b \pmod{m}$“ táknar að a sé samleifa b mátað við m
  - Við segjum að „$a \equiv b \pmod{m}$“ sé samleifing eða leifajafna (congruence) og að m sé leifastofn (modulus) hennar
  - Afleiðing skilgreiningarinnar er að tvær heiltölur eru samleifa mod m þá of því aðeins að þær hafi sama afgang þegar deilt er með m
  - Ef a er ekki samleifa b mátað við m þá skrifum við $a \not\equiv b \pmod{m}$

Samleifa?

- Dæmi: Ákvörðum hvort 17 er samleifa 5 mátað við 6 og hvort 24 og 14 eru samleifa mátuð við 6
- Svar:
  - $17 \equiv 5 \pmod{6}$ vegna þess að 6 gengur upp í $17 - 5 = 12$
  - $24 \not\equiv 14 \pmod{6}$ vegna þess að $24 - 14 = 10$ er ekki deilanlegt með 6

Meira um samleifa

- **Setning:** Látum m vera jákvæða heiltölu. Heiltölurnar a og b eru samleifa mátað við m þá og því aðeins að til sé heiltala k þannig að $a = b + km$
- **Sönnun:**
  - Ef $a \equiv b \ (mod\ m)$ þá (samkvæmt skilgreiningu) er $m \mid a - b$. Þarmeð er til heiltala k þannig að $a - b = km$, og þá $a = b + km$
  - Öfugt, ef til er heiltala k þannig að $a = b + km$, þá er $km = a - b$. Þarmeð $m \mid a - b$ og $a \equiv b \ (mod\ m)$

Sambandið milli „(mod m)“ og „x **mod** m“

- Merkingin á „mod“ í „$a \equiv b \pmod{m}$“ annars vegar og í „$a \bmod m = b$“ hins vegar, er ekki sama
  - Í $a \equiv b \ (mod\ m)$ eru notuð vensl á mengi heiltalna (þ.e. vensl frá $\mathbb{Z}$ til $\mathbb{Z}$)
  - Í $a \bmod m = b$ er verið að nota **mod** sem fall (tvíundaraðgerð)
- Samanber eftirfarandi setningu
- **Setning:** Látum a og b vera heiltölur og látum m vera jákvæða heiltölu. Þá er $a \equiv b \ (mod\ m)$ þá og því aðeins að $a \bmod m = b \bmod m$

Leifar summa og margfelda

- **Setning:** Látum m vera jákvæða heiltölu. Ef

$$a \equiv b \ (mod\ m)$$

og

$$c \equiv d \ (mod\ m)$$

þá

$$a + c \equiv b + c \ (mod\ m)$$

og

$$ac \equiv bc \ (mod\ m)$$

- Dæmi: Þar eð $7 \equiv 2 \ (mod\ 5)$ og $11 \equiv 1 \ (mod\ 5)$ fáum við frá setningu 5 að:

$$18 = 7 + 11 \equiv 2 + 1 = 3 \ (mod\ 5)$$
$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \ (mod\ 5)$$

Algebra (bókstafareikningur) með leifar

- Margföldun báðu megin leifajöfnu viðheldur sanngildi
  - Ef $a \equiv b \ (mod\ m)$ þá gildir $ca \equiv cb \ (mod\ m)$ fyrir hvaða heiltölu c sem er, samkvæmt setningu 5 með $d = c$
- Að leggja heiltölu báðu megin við leifajöfnu viðheldur sanngildi
  - Ef $a \equiv b \ (mod\ m)$ þá gildir $c + a \equiv c + b \ (mod\ m)$ fyrir hvaða heiltölu c sem er, samkvæmt setningu 5 með $d = c$
- Hins vegar getur deiling báðu megin valdið því að sanngildið breytist
  - Dæmi: $14 \equiv 8 \ (mod\ 6)$ er satt, en ef við deilum báðu megin með 2 fáum við annars vegar $\frac{14}{2} = 7$ og hins vegar $\frac{8}{2} = 4$, en $7 \not\equiv 4 \ (mod\ 6)$
  - Undir sumum kringumstæðum er hins vegar í lagi að deila án þess að hætta sé á að sanngildi breytist

Útreikningar á mod fallinu fyrir summur og margfeldi

- **Fylgisetning við setninguna að framan:** Látum m vera jákvæða heiltölu og látum a og b vera heiltölur. Þá gildir:

$$(a + b)\ mod\ m = \big((a\ mod\ m) + (b\ mod\ m)\big)\ mod\ m$$

og

$$ab\ mod\ m = \big((a\ mod\ m)(b\ mod\ m)\big)\ mod\ m$$

Meiri leifareikningar

- **Skilgreiningar:** Fyrir jákvæða heiltölu m Látum $\mathbb{Z}_m$ vera mengið $\{0,1,\dots,m-1\}$
  - Tvíundaraðgerðin (binary operation) $+_m$ er skilgreind sem $a +_m b = (a+b)\ mod\ m$. Þetta er kallað **samlagning mátuð við m** (addition modulo m, **samlagning módúló m**)
  - Tvíundaraðgerðin (binary operation) $\cdot_m$ er skilgreind sem $a \cdot_m b = (a \cdot b)\ mod\ m$. Þetta er kallað **margföldun mátuð við m** (multiplication modulo m, **margföldun módúló m**)
  - Að reikna með þessum aðgerðum kallast að reikna mátað við m (módúló m)
- Dæmi: Reiknum $7 \cdot_{11} 9$ og $7 \cdot_{11} 9$
  - $7 +_{11} 9 = (7+9)\ mod\ 11 = 16\ mod\ 11 = 5$
  - $7 \cdot_{11} 9 = (7 \cdot 9)\ mod\ 11 = 63\ mod\ 11 = 8$

Meiri leifareikningar

- Aðgerðirnar $+_m$ og $\cdot_m$ hafa marga sömu eiginleika og venjuleg samlagning og margföldun
  - **Lokun:** Ef a og b eru í $\mathbb{Z}_m$ þá eru $a +_m b$ og $a \cdot_m b$ einnig í $\mathbb{Z}_m$
  - **Tengiregla:** Ef a, b og c eru í $\mathbb{Z}_m$ þá gilda $(a +_m b) +_m c = a +_m (b +_m c)$ og $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$
  - **Víxlregla:** Ef a og b eru í $\mathbb{Z}_m$ þá gilda $a +_m b = b +_m a$ og $a \cdot_m b = b \cdot_m a$
  - **Hlutleysur:** Gildin 0 og 1 eru hlutleysur fyrir samlagningu og margföldun, þ.e. fyrir öll $a \in \mathbb{Z}_m$:
    - $0 +_m a = a = a +_m 0$
    - $1 \cdot_m a = a \cdot_m 1 = a$

Meiri leifareikningar

- **Samlagningarandhverfur:** Ef $a \neq 0$ er í $\mathbb{Z}_m$ þá er $m - a$ samlagningarandhverfa a, mátað við m, og 0 er sín eigin samlagningarandhverfa
  - $a +_m (m - a) = 0$ og $0 +_m 0 = 0$
- **Dreifiregla:** Ef a, b og c eru í $\mathbb{Z}_m$ þá gildir

$$a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$$
$$(a +_m b) \cdot_m c = a \cdot_m c +_m b \cdot_m c$$

- Við ræðum ekki strax um margföldunarandhverfur því þær eru ekki alltaf til, til dæmis er ekki til margföldunarandhverfa fyrir 2 mátað við 6
- [Á máli stærðfræðinga sem fjalla um algebru segjum við að $\mathbb{Z}_m$ með $+_m$ sé víxlin grúpa (commutative group) og að $\mathbb{Z}_m$ með bæði $+_m$ og $\cdot_m$ sé víxlinn baugur (commutative ring)]

Margföldun með helmingun, tvöföldun og samlagningu

```
{
Notkun:   z := margfalda(x, y)
Fyrir:    x ≥ 0
Eftir:    z er xy þ.e. margfeldi x og y
}
stef margfalda( x, y: heiltölur )
    p := 0; q := y; r := x
    meðan r ≠ 0
        { xy = p + qr }
        ef r er oddatala þá
            p := p + q; r := r − 1
        annars
            r := r/2; q := q + q
    skila p
```

Trúlega elsta algrím sem þekkt er

„Reiknað“ með vogarskálum á steinöld?

Var notað í gömlum örgjörvum

Veldishafning með helmingun, öðru veldi og margföldun

```
{
Notkun:   z := veldi(x, y)
Fyrir:    y ≥ 0
Eftir:    z er x^y þ.e. x í veldi y
}
stef veldi( x, y: heiltölur )
    p := 1; q := x; r := y
    meðan r ≠ 0
        { x^y = p · q^r }
        ef r er oddatala þá
            p := p · q; r := r − 1
        annars
            r := r/2; q := q^2
    skila p
```

Mátuð veldishafning

```
{
Notkun:   z := mátaðveldi(x, y, m)
Fyrir:    m > 0 og 0 ≤ x < m og y ≥ 0
Eftir:    z er x^y mod m
}
stef mátaðveldi( x, y, m: heiltölur )
    p := 1; q := x r := y
    meðan r ≠ 0
        { x^y = p · q^r , r ≥ 0, 0 ≤ p,q < m }
        ef r er oddatala þá
            p := p · q mod m; r := r − 1
        annars
            r := r/2; q := q^2 mod m
    skila p
```

Mátuð veldishafning

$$x^y \bmod m = \begin{cases} 1 & \text{ef } y = 0 \\ \left(x^2\right)^{\frac{y}{2}} \bmod m & \text{ef } y \text{ er slétt tala} \\ x \cdot \left(x^2\right)^{\frac{y-1}{2}} \bmod m & \text{ef } y \text{ er oddatala} \end{cases}$$

Mátuð veldishafning (endurkvæm)

```
{
Notkun:   z := mátaðveldi(x, y, m)
Fyrir:    m > 0 og 0 ≤ x < m og y ≥ 0
Eftir:    z er x^y mod m
}
stef mátaðveldi( x, y, m: heiltölur )
    ef y = 0 þá
        skila 1
    ef y er slétt tala þá
        skila mátaðveldi(x^2 mod m, y/2, m)
    p := mátaðveldi(x^2 mod m, (y − 1)/2, m)
    skila x · p mod m
```

Prímtölur og stærstu samdeilar

- Prímtölur (frumtölur, prime number) og eiginleikar þeirra
- Stærstu samdeilar (greater common divisor, GCD) og minnstu samfeldi (least common multiple, LCM)
- Algrím Evklíðs (the Euclidian algorithm)
- GCD sem línulegar samantektir (linear combinations)

Prímtölur

- **Skilgreining:** Jákvæð heiltala $p > 1$ er sögð vera **prímtala** ef einu jákvæðu þættir tölunnar eru 1 og talan sjálf. Jákvæð heiltala stærri en 1 sem ekki er prímtala er sögð vera **samsett**
- **Dæmi:** Heiltalan 7 er prímtala því einu jákvæðu þættirnir eru 7 og 1, en 9 er samsett því 3 gengur upp í 9.

Prímþáttunarsetningin

- **Frumþáttunarsetning**
  Undirstöðusetning reikningslistarinnar
  Grunnsetning reikningslistarinnar
  The Fundamental Theorem of Arithmetic
- **Setning:** Sérhverja jákvæða heiltölu stærri en 1 má rita á einn og aðeins einn hátt sem margfeldi prímtalna, þar sem prímtölurnar eru ritaðar frá hægri til vinstri í röð sem er ekki minnkandi (hvers vegna þarf skilyrðið „stærri en 1“?)
- Dæmi:
  - $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
  - $641 = 641$
  - $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
  - $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Sía Eratosþenesar

TABLE 1 The Sieve of Eratosthenes.

Integers divisible by 2 other than 2 receive an underline.

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	100

Integers divisible by 3 other than 3 receive an underline.

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	100

Integers divisible by 5 other than 5 receive an underline.

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	100

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

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	100

- Sía Eratosþenesar finnur prímtölur í heildsölu
- Til að athuga fyrir staka heiltölu $n > 1$ hvort hún er prímtala má til dæmis athuga fyrir allar heiltölur i þannig að $1 < i \leq \sqrt{n}$ hvort i gengur upp í n – ef ekki þá er n prímtala

Prímtölurnar eru óendanlega margar

- **Setning:** Það eru til óendanlega margar prímtölur (Evklíð)
- **Sönnun:** Notum **óbeina sönnun**. Gerum ráð fyrir að prímtölurnar séu endanlega margar, $p_1, p_2, \dots, p_n$
- Látum $q = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$
- Þá er afgangurinn þegar q er deilt með p_i alltaf 1, fyrir $i = 1, \dots, n$.
- Engin prímtalnanna gengur því upp í q og q getur því ekki verið samsett tala
- Þá hlýtur q að vera prímtala, en það er þá í **mótsögn** við forsenduna að hægt sé að telja upp endanlega runu $p_1, p_2, \dots, p_n$ af öllum prímtölum

Dreifing prímtalna

- **Prímtölusetningin:** Ef við skilgreinum $\pi(N)$ sem fjölda þeirra prímtalna sem eru $\leq N$ þá gildir

$$\lim_{N\to\infty} \frac{\pi(N)}{\ln(N)} = 1$$

- Afleiðing er að fjöldi prímtalna $\leq N$ er um það bil $\ln(N)$
- Líkindin á því að slembitala $\leq N$ sé prímtala er um það bil $\frac{1}{\ln(N)}$

Stærstu samdeilar

- **Skilgreining:** Látum a og b vera heiltölur, ekki báðar núll. Stærsta heiltala d þannig að $d \mid a$ og $d \mid b$ er kölluð stærsti samdeilir a og b. Stærsti samdeilirinn er táknaður með $\gcd(a, b)$
- Finna má stærsta samdeili smárra talna með því að prófa sig áfram
- **Dæmi:** Hver er stærsti samdeilir 24 og 36?
- **Svar:** $\gcd(24,36) = 12$
- **Dæmi:** Hver er stærsti samdeilir 17 og 22?
- **Svar:** $\gcd(17,22) = 1$

Stærstu samdeilar

- **Skilgreining:** Heiltölur a og b eru sagðar vera **ósamþátta** (relatively prime) hvenær sem $\gcd(a,b) = 1$
- **Dæmi:** 17 og 22
- **Skilgreining:** Heiltölur $a_1, a_2, \ldots, a_n$ eru sagðar vera **innbyrðis ósamþátta** hvenær sem $\gcd(a_i, a_j) = 1$ fyrir öll i og j þannig að $1 \leq i < j \leq n$
- **Dæmi:** Eru 10, 17 og 21 innbyrðis ósamþátta?
- **Svar:** Já, því $\gcd(10,17) = \gcd(10,21) = \gcd(17,21) = 1$
- **Dæmi:** Eru 10, 19 og 24 innbyrðis ósamþátta?
- **Svar:** Nei, því $\gcd(10,24) = 2$

Prímþáttun gefur stærsta samdeili (GCD)

- Gerum ráð fyrir að prímþáttanir a og b séu

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_n^{a_n}, \qquad b = p_1^{b_1} \cdot p_2^{b_2} \cdot \dots \cdot p_n^{b_n},$$

- þar sem sérhvert veldi er ekki-neikvæð heiltala og allar prímtölur sem eru þættir í öðru af a og b eru taldar með í báðum þáttunum.
- Þá gildir:

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \dots \cdot p_n^{\min(a_n, b_n)}$$

- Dæmi: $120 = 2^3 \cdot 3 \cdot 5$, $500 = 2^2 \cdot 5^3$

$$\gcd(120,500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$$

- Þetta er mjög hægvirk aðferð til að finna stærsta samdeili vegna þessa að það er ekki nein þekkt hraðvirk aðferð til að þátta heiltölur

Minnsta samfeldi (minnsti samnefnari, least common multiple, LCM)

- **Skilgreining:** Minnsta samfeldi jákvæðra heiltalna a og b er minnsta jákvæða heiltala sem er deilanleg með bæði a og b. Það er táknað með $lcm(a,b)$
- Reikna má minnsta samfeldi út frá prímþáttun

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ldots \cdot p_n^{\max(a_n,b_n)}$$

- Dæmi: $\operatorname{lcm}(2^3 \cdot 3^5 \cdot 7^2, 2^4 \cdot 3^3) = 2^{\max(3,4)} \cdot 3^{\max(5,3)} \cdot 7^{\max(2,0)} = 2^4 \cdot 3^5 \cdot 7^2$
- Það er einfalt samband milli stærsta samdeilis og minnsta samfeldis
- **Setning:** Látum a og b vera jákvæðar heiltölur. Þá gildir:

$$a \cdot b = \gcd(a,b) \cdot lcm(a,b)$$

Algrím Evklíðs (Euclidean Algorithm)

- Algrím Evklíðs er aðferð til að reikna stærsta samdeili tveggja heiltalna
- Gerum ráð fyrir að a og b séu ekki-neikvæðar heiltölur, ekki báðar núll:

$$\gcd(a,b) = \begin{cases} b & ef\ a = 0 \\ \gcd(b,a) & ef\ a > b \\ \gcd(b-a,a) & ef\ a \leq b \end{cases}$$

- Eða, (mun hraðvirkara, oftast):

$$\gcd(a,b) = \begin{cases} b & ef\ a = 0 \\ \gcd(b,a) & ef\ a > b \\ \gcd(b\ \mathbf{mod}\ a,a) & ef\ a \leq b \end{cases}$$

Algrím Evklíðs

- Dæmi:

$$\gcd(91,287) =$$
$$\gcd(287 \bmod 91,91) =$$
$$\gcd(14,91) =$$
$$\gcd(91 \bmod 14,14) =$$
$$\gcd(7,14) =$$
$$\gcd(14 \bmod 7,7) =$$
$$\gcd(0,7) =$$
$$7$$

Algrím Evklíðs

```
{
Notkun:   c = gcd(a, b)
Fyrir:    a og b eru heiltölur, 0 ≤ a < b
Eftir:    c er stærsti samdeilir a og b
}
stef gcd( a, b: heiltölur )
    x := a
    y := b
    meðan x ≠ 0
        { gcd(a,b) = gcd(x,y), 0 ≤ x < y }
        r := y mod x
        y := x
        x := r
    skila y
```

x	y
91	287
14	91
7	14
0	7

Rökstuðningur algríms Evklíðs

- **Hjálparsetning**: Látum $b = a \cdot q + r$ þar sem a, b, q og r eru heiltölur. Þá er $\gcd(a, b) = \gcd(r, a)$.
- **Sönnun**:
  - Gerum ráð fyrir að d gangi upp í bæði a og b. Þá gengur d einnig upp í $b - a \cdot q = r$ (samkvæmt setningu 1). Þarmeð fæst að allir samdeilar a og b eru einnig samdeilar r og a.
  - Gerum ráð fyrir að d gangi bæði upp í a og r. Þá gengur d einnig upp í $a \cdot q + r = b$. Þarmeð fæst að allir samdeilar a og r eru einnig samdeilar a og b.
- Þarmeð fæst að $\gcd(a, b) = \gcd(r, a)$

GCD sem línuleg samantekt

- Jafna Bézouts: Ef a og b eru jákvæðar heiltölur þá eru til heiltölur s og t þannig að $\gcd(a,b) = sa + tb$
- Skilgreining: Ef a og b eru jákvæðar heiltölur þá kallast tölurnar s og t þannig að $\gcd(a,b) = sa + tb$ Bézout stuðlar a og b. Jafnan $\gcd(a,b) = sa + tb$ kallast jafna Bézouts.
- Dæmi:
  - $\gcd(6,14) = (-2) \cdot 6 + 1 \cdot 14 = 2$
  - $\gcd(91,287) = 19 \cdot 91 + (-6) \cdot 287 = 7$

Útvíkkað Algrím Evklíðs

{
Notkun: evklíð(a, b, s, t)
Fyrir: a og b eru heiltölur, $0 \leq a < b$
Eftir: s og t eru heiltölur þannig að $s \cdot a + t \cdot b$ er stærsti samdeilir a og b
}

stef gcd(a, b: heiltölur; s, t: heiltölubreytur)

$n \coloneqq 1;\ r_0 \coloneqq b;\ r_1 \coloneqq a;\ s_0 \coloneqq 1;\ s_1 \coloneqq 0;\ t_0 \coloneqq 0;\ t_1 \coloneqq 1$

meðan $r_n \neq 0$

$\{\ n \geq 1,\ 0 \leq r_n < r_{n-1}\ \}$

$\{\ \gcd(a,b) = \gcd(r_{n-1}, r_n)\ \}$

$\{\ r_i = s_i \cdot a + t_i \cdot b,\ \text{fyrir } i = 0, \ldots, n\ \}$

$q \coloneqq r_n$ **div** r_{n-1}

$r_{n+1} \coloneqq r_{n-1} - q \cdot r_n$

$s_{n+1} \coloneqq s_{n-1} - q \cdot s_n$

$t_{n+1} \coloneqq t_{n-1} - q \cdot t_n$

$n \coloneqq n + 1$

$s \coloneqq s_{n-1}$

$t \coloneqq t_{n-1}$

Athugið að útvíkkað algrím Evklíðs (með fullum rökstuðningi) er sönnun á jöfnu Bézouts

n	r_n	s_n	t_n
0	287	0	1
1	91	1	0
2	14	-3	1
3	7	19	-6
4	0		

$$\gcd(91,287) = 19 \cdot 91 - 6 \cdot 287 = 7$$

Afleiðingar jöfnu Bézouts

- **Hjálparsetning:** Ef a, b og c eru jákvæðar heiltölur þannig að $\gcd(a,b) = 1$ og $a \mid bc$, þá gildir $a \mid c$.
- **Sönnun:** Gerum ráð fyrir að $\gcd(a,b) = 1$ og $a \mid bc$
  - Þar eð $\gcd(a,b) = 1$ eru samkvæmt setningu Bézouts til heiltölur s og t þannig að $sa + tb = 1$.
  - Margföldum báðu megin með c og fáum $sac + tbc = c$
  - Við sjáum að $a \mid tbc$ (því $a \mid bc$ og tbc er margfeldi bc) og $a \mid sac$ (því sac er margfeldi a) og þarmeð $a \mid (sac + tbc)$
  - Við getum því dregið þá ályktun að $a \mid c$ þar eð $c = sac + tbc$
- **Hjálparsetning:** Ef p er prímtala og $p \mid a_1 a_2 \cdots a_n$ þá $p \mid a_i$ fyrir eitthvert i

Lausnir leifajafna

- Línulegar leifajöfnur (linear congruences)
- Kínverska leifasetningin (The Chinese Remainder Theorem)
- Litla setning Fermats

Línulegar leifajöfnur

- **Skilgreining:** Leifajafna á sniðinu
$$ax \equiv b \ (mod\ m)$$
- þar sem m er jákvæð heiltala, a og b eru heiltölur og x er breyta, er kölluð línuleg leifajafna (linear congruence).
- Lausnir leifajöfnunnar $ax \equiv b \ (mod\ m)$ eru allar heiltölur x sem uppfylla leifajöfnuna.
- **Skilgreining:** Heiltala $\bar{a}$ þannig að $\bar{a} \cdot a \equiv 1 \ (mod\ m)$ er sögð vera **andhverfa** a **mátað við** m (inverse of a modulo m)
- Dæmi: 5 er andhverfa 3 mátað við 7 vegna þess að $5 \cdot 3 = 15 \equiv 1 \ (mod\ 7)$
- Ein leið til að leysa línulegar leifajöfnur er að nota andhverfuna $\bar{a}$, ef hún er til. Þótt við megum ekki deila báðu megin leifajöfnu megum við margfalda með $\bar{a}$ til að einangra x.

Andhverfa a mátað við m

- **Setning:** Ef a og m eru ósamþátta og $m > 1$ þá er til andhverfa a mátað við m. Ennfremur eru allar slíkar andhverfur jafnar, mátað við m.
  - Því er til ein og aðeins ein tala $\bar{a}$ þannig að $0 \leq \bar{a} < m$ og $\bar{a}a \equiv 1\ (mod\ m)$
- **Sönnun:** Þar eð $\gcd(a, m) = 1$ eru til heiltölur s og t þannig að $sa + tm = 1$
  - Þarmeð $sa + tm \equiv 1\ (mod\ m)$
  - Þar eð $tm \equiv 0\ (mod\ m)$ fæst að $sa \equiv 1\ (mod\ m)$
  - Þar með er s andhverfa a mátað við m
  - Allar slíkar andhverfur eru jafnar, mátað við m, en það er ekki sannað hér

Útvíkkaða algrím Evklíðs reiknar andhverfur

Eftir kallið Evklíð(a,m,s,t) inniheldur s andhverfu a mátað við m

Notum andhverfu til að leysa leyfajöfnu

- Almennt getum við leyst leyfajöfnuna $ax \equiv b\ (mod\ m)$ með því að margfalda báðu megin með $\bar{a}$
  - Dæmi: Leysum $3x = 4\ (mod\ m)$
  - Lausn: Við sáum framar að -3 er andhverfa 3 mátað við 7. Margföldum því báðu megin með -3 og fáum $-6x \equiv -8\ (mod\ m)$, sem er jafngilt $x \equiv 6\ (mod\ m)$

Kínverska leifasetningin (The Chinese Remainder Theorem)

- **Setning (kínverska leifasetningin):** Látum $m_1, m_2, \ldots, m_n$ vera innbyrðis ósamþátta jákvæðar heiltölur stærri en einn og látum $a_1, a_2, \ldots, a_n$ vera hvaða heiltölur sem er. Þá hefur leifajöfnukerfið

$$x \equiv a_1 \ (mod\ m_1)$$
$$x \equiv a_2 \ (mod\ m_2)$$
$$\ldots$$
$$x \equiv a_n \ (mod\ m_n)$$

  eina og aðeins eina lausn mátað við $m_1 m_2 \cdots m_n$, þ.e. eina og aðeins eina lausn x þannig að $0 \leq \mathrm{x} < m_1 m_2 \cdots m_n$

Kínverska leifasetningin

- Við munum ekki sanna kínversku leifasetninguna, en við skulum sjá hver **lausnin** er. Látum

$$m = m_1 m_2 \cdots m_n$$

Látum síðan $M_k = \frac{m}{m_k}$. Þar eð $\gcd(m_k, M_k) = 1$ er til heiltala y_k sem er andhverfa M_k mátað við m_k, þ.e. $M_k y_k \equiv 1 \ (mod\ m_k)$. Reiknum því summuna

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$$

- Þá mun $M_j \equiv 0 \ (mod\ m_k)$ hvenær sem $j \neq k$. Það veldur því að þetta x uppfyllir allar leifajöfnurnar á undan.

Litla setning Fermats

- **Setning (litla setning Fermats)**: Ef p er prímtala og a er heiltala sem ekki er deilanleg með p þá er $\mathrm{a}^{\mathrm{p}-1} \equiv 1\ (mod\ p)$. Ennfremur gildir fyrir sérhverja heiltölu a að $a^p \equiv a\ (mod\ p)$
- Dæmi: Reiknum $7^{222}\ mod\ 11$.
- Lausn: Samkvæmt litlu setningu Fermats vitum við að $7^{10} \equiv 1\ (mod\ 11)$. Þarmeð er $(7^{10})^k \equiv 1\ (mod\ 11)$ fyrir allar jákvæðar heiltölur k. Því fæst

$$7^{222} = 7^{22\cdot 10} \cdot 7^2 \equiv 1^{22} \cdot 49 \equiv 5\ (mod\ 11)$$

Frumstæðar rætur (primitive root)

- **Skilgreining:** Frumstæð rót mátað við prímtölu p er heiltala r í $\mathbb{Z}_p$ þannig að sérhver heiltala í $\mathbb{Z}_p$ önnur en núll er veldi af r.
- **Mikilvæg staðreynd:** Það er til frumstæð rót fyrir sérhverja prímtölu.
- Dæmi: 2 er frumstæð rót mátað við prímtöluna 11
- Dæmi: 3 er ekki frumstæð rót mátað við prímtöluna 11

Stakrænir lograr (discrete logarithm)

- Látum p vera prímtölu og r vera frumstæð rót mátað við p. Ef a er heiltala milli 1 og $p-1$ þá er til ein og aðeins ein tala e mátað við p þannig að $r^e = a$.
- Skilgreining: Við köllum töluna e að ofan stakrænan logra a miðað við r og mátað við p. Við skrifum $\log_r(a) = e$.
- **Það er engin þekkt leið til að reikna stakrænan logra á hraðvirkan hátt**

Diffie-Hellman lyklaskipti (key exchange protocol)

- Bæði Adda (eða Alice) og Bobbi (eða Bob) og (allir aðrir) eru sammála um að nota tiltekna risastóra prímtölu p og tiltekna frumstæða rót a mátað við p
- Adda býr til risastóra leynilega slembitölu k_1 og sendir $a^{k_1} \, mod \, p$ til Bobba gegnum opinbera samskiptarás
- Bobbi býr til risastóra leynilega slembitölu k_2 og sendir $a^{k_2} \, mod \, p$ til Öddu gegnum opinbera samskiptarás
- Adda reiknar töluna $\left(a^{k_2} \, mod \, p\right)^{k_1} \, mod \, p \equiv a^{k_1 \cdot k_2} \, (mod \, p)$
- Bobbi reiknar töluna $\left(a^{k_1} \, mod \, p\right)^{k_2} \, mod \, p \equiv a^{k_1 \cdot k_2} \, (mod \, p)$
- Þetta er sama talan og Adda og Bobbi geta notað hana sem sameiginlegan dulritunarlykil fyrir samskipti gegnum opinberu samskiptarásina, en enginn annar getur á auðveldan hátt reiknað lykilinn, jafnvel þótt hann hafi hlerað öll samskipti Öddu og Bobba
- Ef einhverjum tekst að finna aðferð til að reikna stakrænan logra á hraðvirkan hátt þá verður þessi aðferð ótraust

Dreifilyklakerfi

- RSA öryggiskerfi og fleiri (DSA, ElGamal) nota tvo lykla, lyklapör
- Dreifilykill (public key) er opinber og skal vera öllum aðgengilegur
- Einkalykill (private key) er leyndarmál og hver aðili á að halda sínum einkalykli leyndum
- Dreifilykill er notaður til að dulrita skeyti til aðila sem hefur samsvarandi einkalykil
- Einkalykill er notaður til að ráða dulrituð skeyti frá hverjum sem er
- Einkalykill er notaður til að undirrita (auðkenna) skeyti frá þeim sem á þann einkalykil
- Dreifilykill er notaður til að staðfesta undirritun skeyta frá aðila með samsvarandi einkalykil

Bálkadulritunarkerfi (block cipher) og útdráttarkerfi (message digest)

- Kerfi eins og Diffie-Helman, RSA, DSA, ElGamal, eru ekki notuð beint til að dulrita heil skeyti eða undirrita heil skeyti
- Bálkadulritunarkerfi eru mun fljótari að dulrita og ráða stór skeyti, þau nota sama lykil til að dulrita og til að ráða
  - AES, DES, IDEA, RC5, og mörg mörg fleiri
  - Dæmi: Sendum móttakandanum skeyti dulritað með AES ásamt AES lykli dulrituðum með RSA dreifilykli
- Útdráttarkerfi geta á fljótvirkan hátt reiknað útdrátt úr stóru skeyti sem hefur þann eiginleika að næstum ómögulegt er að finna annað skeyti sem hefur sama útdrátt
  - SHA-1, SHA-2, SHA-3, SHA-256, MD5, MD6 og mörg fleiri
  - Dæmi: Sendum móttakandanum skeyti ásamt SHA-256 útdrætti úr skeytinu, undirrituðum með RSA einkalykli
- Allt þetta er að gerast í sífellu í samskiptum okkar yfir Internetið