Kuhunkin kohtaan vastataan siihen TIMissä olevaan laatikkoon, jolla on sama nimi kuin kohdan edessä. **Avustajien käyttö on ankarasti kielletty.** Kurssin aineistoa, muita lähteitä (myös netistä löytyviä), laskimia ja ohjelmia saa käyttää. Laskelmiesi tarkastamiseen kannattaa käyttää sivua `http://users.jyu.fi/%7eava/MathCheck_yleinen.html` Monet tästä PDF-tiedostosta maalaamalla kopioidut kaavat voi pudottaa sinne ja ne kelpaavat syntaksin puolesta sellaisinaan tai pienin muutoksin. Kunkin kohdan maksimipistemäärä on 1. Tentin maksimipistemäärä on 30. Jos tekniikka ei toimi, meilaa `antti.valmari@jyu.fi`

Tarkoittakoon H että Suomi saa hopeaa ja K että Suomi saa kultaa. Ilmaise seuraavat logiikan merkinnöillä.

L1 Suomi saa kultaa tai hopeaa.
$K \vee H$

L2 Suomi saa hopeaa jos ja vain jos Suomi ei saa kultaa.
$H \leftrightarrow \neg K$

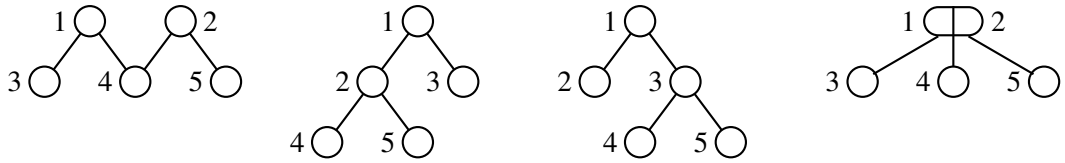
Etukäteen tiedettiin seuraavat. Mitaleita jaetaan täsmälleen kolme: kisojen viimeisen ottelun voittaja saa kultaa ja häviäjä hopeaa, ja toiseksi viimeisen ottelun voittaja saa pronssia. Jokaiseen otteluun osallistuu täsmälleen kaksi maata, joista toinen voittaa ja toinen häviää. Otteluun osallistuvat maat tietenkin tiedetään ennen kuin ottelu alkaa, ja tiedetään myös onko ottelu kisojen viimeinen.

Suomi sai hopeaa ja Saksa ei saanut mitalia.

Tarkastellaan väittämää $Y(x)$: ”jos x voittaa vielä yhdenkin ottelun, niin x saa mitalin”. Esimerkiksi Y(Saksa) oli totta 4.6.2021, jolloin sillä oli jäljellä kaikkiaan kaksi ottelua.

L3 Oliko Y(Suomi) totta juuri ennen kisojen viimeistä ottelua? Perustele vastauksesi.
Kyllä. Jos Suomi voittaa viimeisen ottelun, niin Suomi saa kultaa. Muita otteluita Suomi ei voi enää voittaa, koska muita otteluita ei ole jäljellä.

L4 Oliko Y(Saksa) totta juuri ennen kisojen viimeistä ottelua? Perustele vastauksesi.
Kyllä. Koska Saksa ei saanut kultaa eikä hopeaa, se ei osallistunut viimeiseen otteluun. Siksi juuri ennen viimeistä ottelua Saksalla ei ollut jäljellä enää yhtään ottelua. Niinpä ei ollut mahdollista, että Saksa voittaisi vielä yhden ottelun.



Oletamme, että H on totta, mutta P ja K eivät ole totta.

P1 $P \to H \to K$ tuottaa **T**. Esitä sen lausekepuu valitsemalla jokin kuvista A, B, C tai D ja kertomalla mitä mihinkin solmuun tulee tyyliin A 1:P 2:$\to$ 3:K
C 1: $\to$ 2: P 3: $\to$ 4: H 5: K

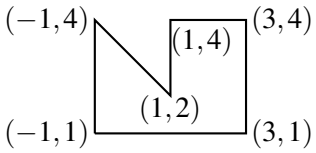
P2 Kirjoita kaava, jossa P, H ja K esiintyvät kukin tasan yhden kerran; $\to$, (ja) esiintyvät niin monta kertaa kuin haluat; ja joka tuottaa **F**. Esitä sen lausekepuu kuten kohdassa P1.
$(P \to H) \to K$
B 1: $\to$ 2: $\to$ 3: K 4: P 5: H

P3 Kirjoita kaava, jossa P, H ja K esiintyvät kukin tasan yhden kerran; $\Rightarrow$ esiintyy kahdesti; ja (ja) esiintyvät niin monta kertaa kuin haluat. Esitä sen lausekepuu kuten edellä.
$P \Rightarrow H \Rightarrow K$
D 1: $\Rightarrow$ 2: $\Rightarrow$ 3: P 4: H 5: K

Kohdissa Y1, Y2, Y3 ja Y4 näytä niin paljon välivaiheita tai selosta ratkaisujasi muulla tavoin niin paljon, että näkyy, että osaisit ratkaista ne ilman muuta apua kuin kynä, paperi ja laskin, jossa on vain yhteen-, vähennys-, kerto- ja jakolasku.

Y1 Kuinka paljon on 1316^{1316} mod 13?
Koska $1316 \bmod 13 = 3$ ja $3^3 \bmod 13 = 27 \bmod 13 = 1$ ja $1316 \bmod 3 = 2$, pätee $1316^{1316} \bmod 13 = 3^{1316} \bmod 13 = 3^2 \bmod 13 = 9$.

Y2 Kirjoita kaava, jonka toteuttavat täsmälleen ne x ja y, joille piste (x,y) on kuvassa olevan viivan sisäpuolella. Kuvassa on annettu kärkipisteet muodossa (x,y). Niitten väliset osuudet ovat suoria.



$-1 < x < 3 \wedge 1 < y < 4 \wedge (x+y < 3 \vee x > 1)$

Y3 Ratkaise yhtälö $(2x+6y+6)(9y-x-7) = 0$.
$\Leftrightarrow\ 2x+6y+6 = 0 \vee 9y-x-7 = 0\ \Leftrightarrow\ x = -3y-3 \vee x = 9y-7$
Minulla sattui ajatusvirhe. Tehtävästä oli tarkoitus tulla yhtälöpari, jonka ratkaisu on $x = -4 \wedge y = \frac{1}{3}$. Tehtävän olisi pitänyt olla esimerkiksi $(2x+6y+6)^2 + (9y-x-7)^2 = 0$. Jotka ratkaisivat yhtälöparin $2x+6y+6 = 0 \wedge 9y-x-7 = 0$ oikein saivat täyden pisteen, ja virheellisistä ratkaisuista vastaavasti vähemmän.

Y4 Ratkaise yhtälö $\dfrac{a-|x-a|+x}{2} = x$.
$\Leftrightarrow\ x < a \wedge a--(x-a)+x = 2x \vee x \geq a \wedge a-(x-a)+x = 2x$
$\Leftrightarrow\ x < a \wedge 2x = 2x \vee x \geq a \wedge 2a = 2x\ \Leftrightarrow\ x \leq a$

BNF-tehtäviä

B1 Esitä ykköstä suurempien luonnollisten lukujen kieli BNF:llä. Luonnollinen luku esitetään numeroiden jonona ilman turhia etunollia. Esimerkiksi `120` ja `2` kuuluvat kieleen, mutta `1` ja `012` eivät kuulu. Anna kielelle nimi K.
K ::= $ML \mid 1DL$
L ::= $\varepsilon \mid LD$
D ::= $0 \mid 1 \mid M$
M ::= $2 \mid 3 \mid 4 \mid 5 \mid 6 \mid 7 \mid 8 \mid 9$

B2 Anna edellisen kohdan kieliopin mukainen jäsennyspuu merkkijonolle `120`. Koska puiden piirtäminen TIM-ikkunaan on hankalaa, esitä vastauksesi seuraavasti. Numeroi solmut siten, että juuri on ykkönen. Kullekin solmulle kirjoita rivi, jossa on ensin solmun numero, sitten solmun sisältö, ja lopuksi lapsisolmujen numerot, siis esimerkiksi 1 X 2 3.
1 K 2 3 4
2 1
3 D 5
4 L 6 7
5 M 8
6 L 9
7 D 10
8 2
9 ε
10 0

B3 Perustele, että B1-kohdan kielioppisi ei tuota merkkijonoa `1`.
Vaihtoehto ML ei voi tuottaa ykkösellä alkavaa merkkijonoa. Vaihtoehto $1DL$ tuottaa ainakin kaksi merkkiä pitkän merkkijonon, koska D ja M tuottavat yhden merkin pituisen merkkijonon.

B4 Kirjoita aliohjelma `tulosta(int a, int b)` joka tulostaa lausekkeen muotoa $ax+b$ ilman turhia osia ja turhia etumerkkejä. Esimerkiksi `tulosta(1, -7)` ei tulosta $1x+-7$ vaan $x-7$. Luvun voi tulostaa komennolla `write(luku);` ja merkkijonon tyyliin `write("Heippa!");`

```
void tulosta( int a, int b ){
  if( a == 0 ){ write( b ); }
  else{
    if( a == -1 ){ write( "-" ); }
    else if( a != 1 ){ write( a ); }
    write( "x" );
    if( b > 0 ){ write( "+" ); }
    if( b != 0 ){ write( b ); }
  }
}
```

B5 Esitä edellisen kohdan tulostuksen kieli BNF:nä. Anna kielelle nimi X. Tehtävän helpottamiseksi oleta, että `int` kattaa kaikki kokonaisluvut ja vain ne. Voit olettaa, että K on valmiiksi määritelty ja tuottaa kohdan B1 mukaisen kielen.
$X ::= 0 \mid B \mid -B \mid A \mid A+B \mid A-B$
$B ::= 1 \mid K$
$A ::= x \mid -x \mid Kx \mid -Kx$

Taulukko $T[1\ldots n]$ indeksoidaan 1:stä n:ään. Esitä seuraavat väittämät kaavoina.

T1 Jossakin kohdassa T:tä on kolmonen.
$\exists i; 1 \le i \le n : T[i] = 3$

T2 Täsmälleen yhdessä kohdassa T:tä on kolmonen.
$\exists i; 1 \le i \le n : T[i] = 3 \wedge \forall j; 1 \le j \le n : i = j \vee T[j] \ne 3$

Muuttujan i arvo on kokonaisluku. Tarkastellaan seuraavaa kaavaa:

$$0 \le i \le n \wedge \forall j; 1 \le j \le i : \exists k; i < k \le n : T[j] = T[k]$$

T3 Anna esimerkki sellaisista n ja T, että kaava on tosi kun $i = 2$.
$n = 3$ ja $T = [0,0,0]$

T4 Jos T on tyhjä, niin millä i:n arvoilla kaava on epätosi? Perustele vastauksesi.
$i \ne 0$. Silloin $\wedge$:n vasen puoli ja samalla koko kaava on epätosi.

T5 Jos T on tyhjä, niin millä i:n arvoilla kaava on tosi? Perustele vastauksesi.
$i = 0$. Silloin $0 \le i \le n$ on tosi ja $\forall$ käy läpi tyhjän välin, joten myös kaavan loppuosa on tosi.

Tästä eteenpäin kaikissa kohdissa oletetaan, että T ei ole tyhjä.

T6 Millä i:n arvoilla kaava saadaan todeksi valitsemalla T:n alkiot sopivasti? Kun $n = 5$, anna esimerkki taulukosta, jolla kaava on tosi mahdollisimman monella i:n arvolla.
$0 \le i < n$. $[0,0,0,0,0]$

T7 Millä sellaisilla i:n arvoilla, että $0 \le i \le n$, kaava on epätosi riippumatta T:n sisällöstä? Perustele vastauksesi.
$i = n$. Silloin $\exists$ käy läpi tyhjän välin ja siksi tuottaa epätosi. Se saa $\forall$-osuuden ja samalla koko kaavan epätodeksi, koska $\forall$ käy läpi epätyhjän välin, koska $n > 0$ koska T on epätyhjä.

T8 Millä i:n arvoilla kaava sanoo, että kaikki T:n alkiot ovat keskenään yhtäsuuret? Perustele vastauksesi.
$i = n-1$. Silloin kaava sanoo, että jokainen muu alkio on yhtäsuuri viimeisen alkion kanssa. Ehto $0 \le i$ toteutuu, koska $n > 0$.

T9 Perustele muille i:n kokonaislukuarvoille kuin mitä vastasit edelliseen kohtaan, että kaava ei sano, että kaikki T:n alkiot ovat keskenään yhtäsuuret.
Jos $i < 0$ tai $i > n$, niin kaava on alkuosansa vuoksi epätosi vaikka kaikki alkiot olisivatkin yhtäsuuret. Jos $i = n$, niin sama tapahtuu T7:n vuoksi. Jos $0 \le i < n-1$, niin kaava on tosi taulukolle jonka muut alkiot ovat 0 mutta viimeinen alkio on 1.

Oheista algoritmia tai sen muunnoksia käytetään muun muassa julkisen avaimen salakirjoituksen avainten luonnissa. Kaikkien muuttujien tyyppi on kokonaisluku. Merkitsemme muuttujien n ja m alkuperäisiä arvoja N ja M. Oletamme, että $N \ge 0$ ja $M \ge 0$. Voidaan todistaa, että aina rivin 2 alussa pätee $n = a_1N + a_2M \wedge m = b_1N + b_2M$.

```
1   a1 := 1;  a2 := 0;  b1 := 0;  b2 := 1;
2   while m ≠ 0 do
3       d := n div m;
4       k := a1 − d · b1;  a1 := b1;  b1 := k;
5       k := a2 − d · b2;  a2 := b2;  b2 := k;
6       k := n mod m;  n := m;  m := k;
```

O1 Mitä kurssin viikkoharjoituksissa käsiteltyä algoritmia yllä oleva algoritmi muistuttaa?
Suurimman yhteisen tekijän algoritmia eli modernia Eukleideen algoritmia.

O2 Mitä on muuttujassa n kun yllä oleva algoritmi lopettaa? Ilmaise vastaus muuttujien alkuperäisten arvojen funktiona.
$\gcd(N, M)$

O3 Perustele edellisen kohdan vastauksesi. Perustelussa saa käyttää kaikkea mitä kurssilla on kerrottu kohdassa O1 mainitusta algoritmista. Kohdassa O1 mainitun algoritmin ominaisuuksia ei tarvitse perustella.
Rivien 1, 3, 4 ja 5 poistaminen ei vaikuta algoritmin yleiseen kulkuun eikä muuttujien n ja m saamiin arvoihin. Siksi n:n arvo lopussa on sama kuin mikä se olisi, jos rivit 1, 3, 4 ja 5 olisi poistettu. Niiden poistaminen muuttaa algoritmin moderniksi Eukleideen algoritmiksi. Siksi n:n arvo lopussa on n:n ja m:n alkuperäisten arvojen suurin yhteinen tekijä.

O4 Anna kaava, joka on voimassa aina rivin 5 lopussa ja ilmaisee m:n arvon N:n, M:n ja mahdollisesti muiden muuttujien avulla. Perustele kaavasi vetoamalla tilanteeseen, joka vallitsi kun oltiin edellisen kerran rivillä 2.
$m = a_1N + a_2M$
Rivin 2 alussa päti $m = b_1N + b_2M$. Sen jälkeen a_1 sai arvonsa b_1:stä ja a_2 b_2:sta, ja m, N ja M eivät ole muuttuneet.

O5 Anna kaava, joka on voimassa aina rivin 6 lopussa ja ilmaisee k:n arvon N:n, M:n ja mahdollisesti muiden muuttujien avulla. Kaava ei saa käyttää m:ää. Perustele kaavasi vetoamalla tilanteeseen, joka vallitsi kun oltiin edellisen kerran rivillä 2.
$k = b_1N + b_2M$
Muuttujien arvoilla rivin 4 alussa päti $n \bmod m = n - m(n \operatorname{div} m) = n - md = a_1N + a_2M - d(b_1N - b_2M) = (a_1 - db_1)N + (a_2 - db_2)M$. Rivin 4 alun $n \bmod m$, $a_1 - db_1$ ja $a_2 - db_2$ ovat yhtäsuuria rivin 6 lopun k:n, b_1:n ja b_2:n kanssa.

loppu