802328A LUKUTEORIAN PERUSTEET OSA I
BASICS OF NUMBER THEORY PART I

Tapani Matala-aho

MATEMATIIKKA/LUTK/OULUN YLIOPISTO

SYKSY 2018

LUKUTEORIA, NUMBER THEORY, THÉORIE DES NOMBRES

Lukuteoria eli aritmetiikka tutkii erityisesti kokonaislukuihin liittyviä kysymyksiä. Aritmetiikan määritelmästä: Ensinnäkin, alkeisaritmetiikka eli alkeismatematiikka voidaan käsittää kokonaislukujen ja niiden laskutoimitusten-yhteenlasku, vähennyslasku, kertolasku ja jakolasku-muodostamaksi järjestelmäksi. Esimerkiksi korttipeli voidaan ajatella matemaattiseksi järjestelmäksi, jossa lukuja vastaavat kortit ja laskutoimituksia pelin säännöt. Toisaalta aritmetiikka laajasti katsottuna sisältää myös tutkimukselliset kysymykset ja niiden tarkasteluun kehitetyt työkalut. Tällöin termit lukuteoria ja aritmetiikka samaistetaan-kuten voi nähdä alan päälehtien Acta Arithmetica ja Journal of Number Theory nimistä.
ARITHMETIC in Wikipedia/LINK.
NUMBER THEORY in Wikipedia/LINK.

LUKUJA SEKÄ TYÖKALUJA

802328A Lukuteorian perusteet (5 op) [=Aikaisempi Lukuteoria I (5op)]

LUKUJA SEKÄ TYÖKALUJA

802328A Lukuteorian perusteet (5 op) [=Aikaisempi Lukuteoria I (5op)]

Luennoilla tarkastelemme matematiikan ja erityisesti lukuteorian tutkimuksessa usein esiintyvien lukujen aritmeettisia ominaisuuksia sekä aiheeseen liittyviä menetelmiä. Tutkittavia lukuja ovat esimerkiksi binomikertoimet, ketjumurtoluvut, potenssisummat sekä eräät matemaatikkojen Euler, Fermat, Fibonacci, Heron, Lucas, Neper, Pythagoras, Wilson ja Wolstenholme mukaan nimitetyt luvut ja käsitteet. Sovellettavista työkaluista mainittakoon generoivat sarjat, irrationaalisuustarkastelut, matriisiesitykset, rationaalilukujen ja polynomien kongruenssit, rekursiot ja teleskoopit.
802328A Lukuteorian perusteet/NOPPA-LINK.

NUMBERS AND TOOLS

In our lectures we consider arithmetical properties of the common numbers involved in studing mathematics and in particular number theory. Also the methods will get a special interest. Examples of the numbers under the research will be binomials, continued fractions, sums of powers and some numbers sharing a name with the mathematicians Euler, Fermat, Fibonacci, Heron, Lucas, Neper, Pythagoras, Wilson and Wolstenholme. From the tools we mention congruences of rational numbers and polynomials, generating series, irrationality considerations, matrix presentations, recurrences and telescopes.
802328A Basics in Number Theory/NOPPA-LINK.

BASICS AND REFERENCES/POHJATIEDOT JA LÄHTEITÄ

Pohjatietoina oletetaan 1. vuoden kurssit, erityisesti:
802354A Algebran perusteet/LINK, sekä
802355A Algebralliset rakenteet/LINK.

BASICS AND REFERENCES/POHJATIEDOT JA LÄHTEITÄ

Pohjatietoina oletetaan 1. vuoden kurssit, erityisesti:
802354A Algebran perusteet/LINK, sekä
802355A Algebralliset rakenteet/LINK.

Aluksi tosin kerrataan nopesti ilman todistuksia kurssin Algebran perusteet jaollisuuteen ja kongruenssiin liittyviä tuloksia, kappaleessa 4.

BASICS AND REFERENCES/POHJATIEDOT JA LÄHTEITÄ

Pohjatietoina oletetaan 1. vuoden kurssit, erityisesti:
802354A Algebran perusteet/LINK, sekä
802355A Algebralliset rakenteet/LINK.

Aluksi tosin kerrataan nopesti ilman todistuksia kurssin Algebran perusteet jaollisuuteen ja kongruenssiin liittyviä tuloksia, kappaleessa 4.

LÄHTEITÄ:
G.H. Hardy & E.M. Wright: An Introduction to the Theory of Numbers.
Kenneth H. Rosen: Elementary number theory and its applications.
Number Theory Web/LINK
American Mathematical Monthly/LINK

Määritelmä 1

Floor function/ Lattiafunktio (eli porrasfunktio)

$$\lfloor\ \rfloor : \mathbb{R} \to \mathbb{Z}$$

is given by setting

$$\lfloor x \rfloor = [x] = \max\{n \in \mathbb{Z} \mid n \leqslant x\}$$

for all $x \in \mathbb{R}$.

Esimerkki 1

If $x \in \mathbb{R}_{\geq 0}$, *then* $\lfloor x \rfloor$ *is the integer part/kokonaisosa of* x, *but e.g.*

$$\lfloor -1.2 \rfloor = -2.$$

Määritelmä 2

Ceiling function/Kattofunktio

$$\lceil \ \rceil : \mathbb{R} \to \mathbb{Z}$$

saadaan asettamalla

$$\lceil x \rceil = \min\{n \in \mathbb{Z} \mid x \leq n\}$$

aina, kun $x \in \mathbb{R}$.

Esimerkki 2

$$\lceil -1.2 \rceil = -1.$$

Lause 1

Let $x \in \mathbb{R}$ be given in the form

$$x = k + c, \quad k \in \mathbb{Z},\ 0 \leq c < 1. \tag{3.1}$$

Then

$$k = \lfloor x \rfloor. \tag{3.2}$$

Further

$$\lceil x \rceil = -\lfloor -x \rfloor \quad \forall x \in \mathbb{R}, \tag{3.3}$$

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \quad \forall x \in \mathbb{R} \tag{3.4}$$

$$\lfloor x + k \rfloor = \lfloor x \rfloor + k \quad \forall x \in \mathbb{R}, \forall k \in \mathbb{Z}, \tag{3.5}$$

$$\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \quad \forall x, y \in \mathbb{R}, \tag{3.6}$$

$$\lfloor x \rfloor \lfloor y \rfloor \leq \lfloor xy \rfloor \quad \forall x, y \in \mathbb{R}_{\geq 0}. \tag{3.7}$$

Proof of Case (3.2)

We shall use the ordering properties of real numbers.
Let us start by denoting

$$m := \lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leqslant x\}. \tag{3.8}$$

Thus

$$m \leq x < m+1 \quad \Rightarrow \quad m \leq k+c < m+1 \quad \Rightarrow \tag{3.9}$$

$$m \leq k+c < k+1 \quad \Rightarrow \quad m \leq k \tag{3.10}$$

$$k < m+1-c \leq m+1 \quad \Rightarrow \quad k \leq m. \tag{3.11}$$

Hence

$$k = m = \lfloor x \rfloor. \quad \square$$

Merkintä 1

$$\{x\} = x - \lfloor x \rfloor. \tag{3.12}$$

We note, that

$$0 \leq \{x\} < 1 \tag{3.13}$$

and $\{x\}$ gives the decimal part of positive $x \in \mathbb{R}^+$.

Esimerkki 3

$$\{1.2\} = 0.2 \tag{3.14}$$

but

$$\{-1.2\} = 0.8 \tag{3.15}$$

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}; \tag{3.16}$$

$$\sum_{k=0}^{n} a^k = \frac{a^{n+1}-1}{a-1}, \quad a \neq 1; \tag{3.17}$$

$$\sum_{k=0}^{n} \binom{n}{k} t^k = (1+t)^n, \quad n \in \mathbb{N}. \tag{3.18}$$

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1). \tag{3.19}$$

$$a^n + 1 = (a+1)(a^{n-1} - a^{n-2} + \cdots - a + 1), \quad 2 \nmid n. \tag{3.20}$$

$$A^n - B^n = (A-B)(A^{n-1} + A^{n-2}B + \cdots + AB^{n-2} + B^{n-1}). \tag{3.21}$$

Proof of (3.17)

By

$$a^k = 1 \cdot a^k = \frac{a-1}{a-1} a^k = \frac{a^{k+1} - a^k}{a-1}, \quad a \neq 1; \tag{3.22}$$

we get

$$\sum_{k=0}^{n} a^k = \frac{1}{a-1} \sum_{k=0}^{n} (a^{k+1} - a^k) =$$

$$\frac{1}{a-1}(a^{n+1} - a^n + a^n - a^{n-1} + \ldots a^2 - a^1 + a^1 - a^0) = \frac{a^{n+1} - 1}{a-1}. \quad \square \tag{3.23}$$

This proof is an example of the idea of telescoping series.

DIVISIBILITY/Jaollisuus

Määritelmä 3

Let $a, b \in \mathbb{Z}$. Then

$$b|a \quad \Leftrightarrow \quad \exists c \in \mathbb{Z}: \quad a = bc. \tag{4.1}$$

When $b|a$, then b divides/jakaa a or

DIVISIBILITY/Jaollisuus

Määritelmä 3

Let $a, b \in \mathbb{Z}$. Then

$$b|a \quad \Leftrightarrow \quad \exists c \in \mathbb{Z}: \quad a = bc. \tag{4.1}$$

When $b|a$, then b divides/jakaa a or

b is a factor/tekijä of a or

DIVISIBILITY/Jaollisuus

Määritelmä 3

Let $a, b \in \mathbb{Z}$. Then

$$b|a \quad \Leftrightarrow \quad \exists c \in \mathbb{Z}: \quad a = bc. \tag{4.1}$$

When $b|a$, then b divides/jakaa a or

b is a factor/tekijä of a or

a is a multiple/monikerta of b.

DIVISIBILITY/Jaollisuus

Määritelmä 3

Let $a, b \in \mathbb{Z}$. Then

$$b|a \quad \Leftrightarrow \quad \exists c \in \mathbb{Z}: \quad a = bc. \tag{4.1}$$

When $b|a$, then b divides/jakaa a or

b is a factor/tekijä of a or

a is a multiple/monikerta of b.

The notation $b \nmid a$ will be used, when b does not divide/ei jaa a.

DIVISIBILITY/Jaollisuus

Määritelmä 3

Let $a, b \in \mathbb{Z}$. Then

$$b|a \quad \Leftrightarrow \quad \exists c \in \mathbb{Z}: \quad a = bc. \tag{4.1}$$

When $b|a$, then b divides/jakaa a or

b is a factor/tekijä of a or

a is a multiple/monikerta of b.

The notation $b \nmid a$ will be used, when b does not divide/ei jaa a.

Esimerkki 4

$$0|0, \quad 0 \nmid a \neq 0. \tag{4.2}$$

Divisibility rules/Jaollisuuden laskusääntöjä

Lause 2

Let/Olkoot $k, m, n, r, s \in \mathbb{Z}$. Then/Tällöin

Divisibility rules/Jaollisuuden laskusääntöjä

Lause 2

Let/Olkoot $k, m, n, r, s \in \mathbb{Z}$. Then/Tällöin

$$\pm 1 | k, \quad \pm k | k; \tag{4.3}$$

Divisibility rules/Jaollisuuden laskusääntöjä

Lause 2

Let/Olkoot $k, m, n, r, s \in \mathbb{Z}$. Then/Tällöin

$$\pm 1 | k, \quad \pm k | k; \tag{4.3}$$

$$0 | k \quad \Rightarrow \quad k = 0; \tag{4.4}$$

Divisibility rules/Jaollisuuden laskusääntöjä

Lause 2

Let/Olkoot $k, m, n, r, s \in \mathbb{Z}$. Then/Tällöin

$$\pm 1 | k, \quad \pm k | k; \tag{4.3}$$

$$0 | k \quad \Rightarrow \quad k = 0; \tag{4.4}$$

$$k | 0; \tag{4.5}$$

Divisibility rules/Jaollisuuden laskusääntöjä

Lause 2

Let/Olkoot $k, m, n, r, s \in \mathbb{Z}$. Then/Tällöin

$$\pm 1 | k, \quad \pm k | k; \tag{4.3}$$

$$0 | k \quad \Rightarrow \quad k = 0; \tag{4.4}$$

$$k | 0; \tag{4.5}$$

$$k | 1 \quad \Rightarrow \quad k = \pm 1; \tag{4.6}$$

Divisibility rules/Jaollisuuden laskusääntöjä

Lause 2

Let/Olkoot $k, m, n, r, s \in \mathbb{Z}$. Then/Tällöin

$$\pm 1 | k, \quad \pm k | k; \tag{4.3}$$

$$0 | k \quad \Rightarrow \quad k = 0; \tag{4.4}$$

$$k | 0; \tag{4.5}$$

$$k | 1 \quad \Rightarrow \quad k = \pm 1; \tag{4.6}$$

$$m | n, n | m \quad \Rightarrow \quad n = \pm m; \tag{4.7}$$

Divisibility rules/Jaollisuuden laskusääntöjä

$$k|m,\ \ m|n \quad \Rightarrow \quad k|n; \tag{4.8}$$

Divisibility rules/Jaollisuuden laskusääntöjä

$$k|m,\ m|n \quad \Rightarrow \quad k|n; \tag{4.8}$$

$$k|m, k|n \quad \Rightarrow \quad k|rm + sn; \tag{4.9}$$

Divisibility rules/Jaollisuuden laskusääntöjä

$$k|m,\ m|n \quad \Rightarrow \quad k|n; \tag{4.8}$$

$$k|m, k|n \quad \Rightarrow \quad k|rm + sn; \tag{4.9}$$

$$k|m, k|n \quad \Rightarrow \quad k|m \pm n; \tag{4.10}$$

Divisibility rules/Jaollisuuden laskusääntöjä

$$k|m,\ m|n \quad \Rightarrow \quad k|n; \tag{4.8}$$

$$k|m, k|n \quad \Rightarrow \quad k|rm + sn; \tag{4.9}$$

$$k|m, k|n \quad \Rightarrow \quad k|m \pm n; \tag{4.10}$$

$$k|m, k|n \quad \Rightarrow \quad k^2|mn; \tag{4.11}$$

Divisibility rules/Jaollisuuden laskusääntöjä

$$k|m,\ m|n \quad \Rightarrow \quad k|n; \tag{4.8}$$

$$k|m, k|n \quad \Rightarrow \quad k|rm + sn; \tag{4.9}$$

$$k|m, k|n \quad \Rightarrow \quad k|m \pm n; \tag{4.10}$$

$$k|m, k|n \quad \Rightarrow \quad k^2|mn; \tag{4.11}$$

$$k|m \quad \Rightarrow \quad k|m^h, \quad k^h|m^h, \quad \forall h \in \mathbb{Z}^+ \tag{4.12}$$

Divisibility rules

Huomautus 1

Edellä olevat tulokset voi todistaa suoraan määritelmästä kokonaislukujen kokonaisalue- ja rengasominaisuuksilla.

Divisibility rules

Huomautus 1

Edellä olevat tulokset voi todistaa suoraan määritelmästä kokonaislukujen kokonaisalue- ja rengasominaisuuksilla.
Poikkeus: Sääntö 4.6 otetaan aksiomiksi (tässä vaiheessa), sillä sen todistamiseen tarvitaan itseisarvon ja järjestyksen ominaisuuksia. Katso myöhemmin esitettävä renkaan yksikköryhmä.

Divisibility rules

Huomautus 1

Edellä olevat tulokset voi todistaa suoraan määritelmästä kokonaislukujen kokonaisalue- ja rengasominaisuuksilla.
Poikkeus: Sääntö 4.6 otetaan aksiomiksi (tässä vaiheessa), sillä sen todistamiseen tarvitaan itseisarvon ja järjestyksen ominaisuuksia. Katso myöhemmin esitettävä renkaan yksikköryhmä.

The above results can be proven directly from the definition using the integral domain and ring properties of integers.

Divisibility rules

Huomautus 1

Edellä olevat tulokset voi todistaa suoraan määritelmästä kokonaislukujen kokonaisalue- ja rengasominaisuuksilla.
Poikkeus: Sääntö 4.6 otetaan aksiomiksi (tässä vaiheessa), sillä sen todistamiseen tarvitaan itseisarvon ja järjestyksen ominaisuuksia. Katso myöhemmin esitettävä renkaan yksikköryhmä.

The above results can be proven directly from the definition using the integral domain and ring properties of integers.
An exception: The rule 4.6 is taken as an axiom (at this point) because to prove it we need the properties of absolute values and ordering. It is connected to the unit group of a ring.

Proof. Case (4.7): From the conditions $m|n|m$ we get

$$n = hm = hln \quad h, l \in \mathbb{Z}. \tag{4.13}$$

Case $n \neq 0$. Then

$$(1 - hl)n = 0 \quad \Rightarrow \quad hl = 1 \quad \Rightarrow \quad h = l = \pm 1 \tag{4.14}$$

$$\Rightarrow \quad n = \pm m. \tag{4.15}$$

Tapaus $n = 0$. Because $n|m$, we have

$$0|m \quad \Rightarrow \quad m = 0 \quad \Rightarrow \quad n = \pm m. \quad \square \tag{4.16}$$

Merkintä 2

Olkoot $d, n \in \mathbb{Z}, d \geq 2$, tällöin

$$d^s || n \Leftrightarrow d^s | n \text{ ja } d^{s+1} \nmid n, \quad s \in \mathbb{N}. \tag{4.17}$$

Merkintä 3

Olkoon $k \in \mathbb{Z}$, tällöin

$$k\mathbb{Z} = \{ka | \ a \in \mathbb{Z}\} = \tag{4.18}$$

the set of integers divisible by k/ k:lla jaollisten kokonaislukujen joukko or the multiples of k/eli k:n monikerrat.

Esimerkki 5

$$3^4||162, \quad 1\mathbb{Z} = \mathbb{Z}, \quad 0\mathbb{Z} = \{0\}. \tag{4.19}$$

Määritelmä 4

Let/Olkoon $q \in \mathbb{Z}$ *be given/annettu ja olkoon* $d|q$, $d \in \mathbb{Z}$. *If/Jos* $d \in \{1, -1, q, -q\}$, *then/niin* d *is a trivial factor of the integer* q*/luvun* q *triviaali tekijä. Jos* $d \notin \{1, -1, q, -q\}$, *niin* d *on luvun* q *proper factor/aito tekijä.*

Määritelmä 5

Luku $q \in \mathbb{Z}$ on irreducible/jaoton $\Leftrightarrow$ Jos $d|q$, niin $d = \pm 1$ tai $d = \pm q$.

Thus the irreducible integer q has only trivial factors/siten jaottomalla kokonaisluvulla q on vain triviaalit tekijät. $1, -1, q, -q$.

Määritelmä 6

Luku $p \in \mathbb{Z}$, $p \geq 2$ on prime/alkuluku $\Leftrightarrow$
Jos $d|p$, niin $d = \pm 1$ tai $d = \pm p$.

Merkintä 4

The set of primes/alkulukujen joukko

$$\mathbb{P} = \{p|\ p \text{ on alkuluku}\}.$$

Siten $p \in \mathbb{P} \Leftrightarrow p$ on jaoton ja $p \geq 2$, joten

$$\mathbb{P} = \{p|\ 2, 3, 5, 7, 11, ..., 101, ...\}.$$

Alkutekijä=alkulukutekijä=prime factor.

Määritelmä 7

Luku $n \in \mathbb{Z}$, on composite number/yhdistetty luku $\Leftrightarrow$
on olemassa sellaiset/there exist $r, s \in \mathbb{Z}$, että/such that

$$rs|n; \tag{4.20}$$
$$2 \leq r; \tag{4.21}$$
$$2 \leq s. \tag{4.22}$$

Yhdistetyn luvun määritelmä voidaan antaa myös seuraavassa muodossa.

Määritelmä 8

Luku $n \in \mathbb{Z}$, on composite number/yhdistetty luku $\Leftrightarrow$
n has at least 2 prime factors/n:llä on ainakin 2 alkutekijää.

Esimerkki 6

-4 *on yhdistetty/is composite.*
0 *on yhdistetty.*
-3 *is not composite neither prime but it is irreducible/ei ole yhdistetty eikä alkuluku mutta on jaoton.*

Määritelmä 9

Luvun $n \in \mathbb{Z}_{\geq 2}$ *esitys*

$$n = p_1^{r_1} \cdots p_t^{r_t}, \quad p_i \in \mathbb{P}, \quad r_i \in \mathbb{Z}^+ \tag{4.23}$$

on luvun n luonnollinen alkulukuesitys, alkutekijäesitys, prime factorization, (kanoninen alkutekijähajotelma).

Jos, $m/n \in \mathbb{Q}^*$, niin

$$\frac{m}{n} = p_0^{r_0} p_1^{r_1} \cdots p_t^{r_t}, \quad p_i \in \mathbb{P}, \quad p_0 = -1 \quad r_i \in \mathbb{Z}. \tag{4.24}$$

Esimerkki 7

$$-1 = (-1)^1 2^0 3^0, \quad \frac{40}{128} = \frac{2^3 5}{2^7} = 2^{-4} 5^1 \tag{4.25}$$

Välillä $[1, x]$ olevien d:llä jaollisten kokonaislukujen lukumäärä

Lemma 1

Olkoon $d \in \mathbb{Z}^+$ annettu. Tällöin

$$\#\{k \in \mathbb{Z}^+ |\ 1 \leq k \leq x,\ d|k\} = \left\lfloor \frac{x}{d} \right\rfloor \tag{4.26}$$

Todistus. Ehto $d|k$ kirjoitetaan muodossa $k = k_a = da$, $a \in \mathbb{Z}^+$. Siten

$$\#\{k \in \mathbb{Z}^+ |\ 1 \leq k \leq x,\ d|k\} = \tag{4.27}$$
$$\#\{k_a \in \mathbb{Z}^+ |\ 1 \leq k_a \leq x\} = \tag{4.28}$$
$$\#\{a \in \mathbb{Z}^+ |\ 1 \leq da \leq x\} = \tag{4.29}$$
$$\#\{a \in \mathbb{Z}^+ |\ 1 \leq a \leq x/d\} = \tag{4.30}$$
$$\#\{a \in \mathbb{Z}^+ |\ 1 \leq a \leq \left\lfloor \frac{x}{d} \right\rfloor\} = \left\lfloor \frac{x}{d} \right\rfloor. \quad \square \tag{4.31}$$

Jakoalgoritmi

Lause 3

Olkoot $a, b \in \mathbb{Z}$ *ja* $b \neq 0$. *Tällöin*

$$\exists! \quad q \in \mathbb{Z} \quad ja \quad \exists! \quad r \in \mathbb{N}:$$

$$a = qb + r, \quad 0 \leq r < |b|. \tag{4.32}$$

Kun $b \in \mathbb{Z}^+$, *niin*

$$q = \left\lfloor \frac{a}{b} \right\rfloor. \tag{4.33}$$

Jakoalgoritmi

Lause 3

Olkoot $a, b \in \mathbb{Z}$ *ja* $b \neq 0$. *Tällöin*

$$\exists! \quad q \in \mathbb{Z} \quad ja \quad \exists! \quad r \in \mathbb{N}:$$

$$a = qb + r, \quad 0 \leq r < |b|. \tag{4.32}$$

Kun $b \in \mathbb{Z}^+$, *niin*

$$q = \left\lfloor \frac{a}{b} \right\rfloor. \tag{4.33}$$

Määritelmä 10

Jaettaessa luku a luvulla b, on jakoalgoritmista saatu luku

Jakoalgoritmi

Lause 3

Olkoot $a, b \in \mathbb{Z}$ *ja* $b \neq 0$. *Tällöin*

$$\exists! \quad q \in \mathbb{Z} \quad ja \quad \exists! \quad r \in \mathbb{N}:$$

$$a = qb + r, \quad 0 \leq r < |b|. \tag{4.32}$$

Kun $b \in \mathbb{Z}^+$, *niin*

$$q = \left\lfloor \frac{a}{b} \right\rfloor. \tag{4.33}$$

Määritelmä 10

Jaettaessa luku a luvulla b, on jakoalgoritmista saatu luku r jakojäännös/ remainder ja

Jakoalgoritmi

Lause 3

Olkoot $a, b \in \mathbb{Z}$ *ja* $b \neq 0$. *Tällöin*

$$\exists! \quad q \in \mathbb{Z} \quad ja \quad \exists! \quad r \in \mathbb{N}:$$

$$a = qb + r, \quad 0 \leq r < |b|. \tag{4.32}$$

Kun $b \in \mathbb{Z}^+$, *niin*

$$q = \left\lfloor \frac{a}{b} \right\rfloor. \tag{4.33}$$

Määritelmä 10

Jaettaessa luku a *luvulla* b, *on jakoalgoritmista saatu luku* r *jakojäännös/ remainder ja osamäärän/quotient* a/b

Jakoalgoritmi

Lause 3

Olkoot $a, b \in \mathbb{Z}$ *ja* $b \neq 0$. *Tällöin*

$$\exists! \quad q \in \mathbb{Z} \quad ja \quad \exists! \quad r \in \mathbb{N}:$$

$$a = qb + r, \quad 0 \leq r < |b|. \tag{4.32}$$

Kun $b \in \mathbb{Z}^+$, *niin*

$$q = \left\lfloor \frac{a}{b} \right\rfloor. \tag{4.33}$$

Määritelmä 10

Jaettaessa luku a luvulla b, on jakoalgoritmista saatu luku
r jakojäännös/ remainder ja
osamäärän/quotient a/b
kokonaisosa/integral part on luku q, kun $a/b \geq 0$ *ja* $b \geq 1$.

Osoitetaan tulos: Kun $b \in \mathbb{Z}^+$, niin

$$q = \left\lfloor \frac{a}{b} \right\rfloor . \tag{4.34}$$

Jakoalgoritmin (4.32) nojalla

$$\frac{a}{b} = q + \frac{r}{b}, \quad 0 \leq r \leq b-1 \quad \Rightarrow \quad 0 \leq \frac{r}{b} < 1, \tag{4.35}$$

joten a/b:n kokonaisosa on q. □

Esimerkki 8

$b = 3$,

$$a = -13 = (-5) \cdot 3 + 2, \quad q = -5, \ r = 2, \quad \left\lfloor \frac{a}{b} \right\rfloor = -5 \tag{4.36}$$

$$a = 13 = 4 \cdot 3 + 1, \quad q = 4, \ r = 1, \quad \left\lfloor \frac{a}{b} \right\rfloor = 4 \tag{4.37}$$

Määritelmä 11

Olkoot $a, b \in \mathbb{Z}$ annettu. Tällöin luku $d \in \mathbb{N}$ on lukujen a ja b suurin yhteinen tekijä/greatest common divisor eli
$d = gcd(a, b) = syt(a, b) = (a, b)$ provided/mikäli

$$\begin{array}{llll} d|a & ja & d|b; & [C.D.] \\ c|a & ja & c|b \quad \Rightarrow \quad c|d. & [G.] \end{array}$$

If/Jos $(a, b) = 1$, then we say that/niin sanotaan, että a ja b are relatively prime/ ovat keskenään jaottomia and we use the notation/ja merkitään $a \perp b$.

Huomautus 2

Quite often there exists a definition with $d \in \mathbb{Z}^+$/ Usein esiintyy myös määritelmä, jossa vaaditaan, että $d \in \mathbb{Z}^+$, whereupon/jolloin $(0,0)$ $\nexists$ (Otherwise the same results/Muutoin saadaan samat tulokset).

Esimerkki 9

$$23 \perp 32 \quad \Leftrightarrow (23, 32) = 1 \tag{4.38}$$

Esimerkki 10

$$(0, a) = |a| \quad \forall a \in \mathbb{Z}, \tag{4.39}$$

in particular/erityisesti

$$(0, 0) = 0. \tag{4.40}$$

Lemma 2

Let $p \in \mathbb{P}$, $b \in \mathbb{Z}$. If $p \not| b$, then $p \perp b$.

Proof. If on the contrary $d = (p, b) \geq 2$, then

$$d|p \quad \text{and} \quad d|b \quad \Rightarrow \quad d = p \quad \Rightarrow \quad p|b. \tag{4.41}$$

A contradiction. □

Määritelmä 12

Olkoot $a, b \in \mathbb{Z}$ annettu. Tällöin luku $f \in \mathbb{N}$ on lukujen a ja b pienin yhteinen jaettava/least common multiple eli/or $f = lcm[a, b] = pyj[a, b] = [a, b]$ provided/mikäli

$$\begin{array}{llll} a|f & ja & b|f; & [YJ] \\ a|g & ja & b|g \quad \Rightarrow \quad f|g. & [P] \end{array}$$

Esimerkki 11

$$[0, 0] = 0 \tag{4.42}$$

Lause 4

Olkoot

$$a = \prod_{i=1}^{m} p_i^{r_i}, \quad b = \prod_{i=1}^{m} p_i^{s_i}, \quad p_i \in \mathbb{P}, \ r_i, s_i \in \mathbb{N}.$$

Tällöin

$$gcd(a,b) = syt(a,b) = \prod_{i=1}^{m} p_i^{\min(r_i,s_i)}, \tag{4.43}$$

$$lcm[a,b] = pyj[a,b] = \prod_{i=1}^{m} p_i^{\max(r_i,s_i)}. \tag{4.44}$$

Esimerkki 12

Olkoot $a = 3 \cdot 5^2 \cdot 7, \quad b = 3^2 \cdot 5 \cdot 7$, *nyt*

$$syt(a,b)pyj[a,b] = 3 \cdot 5 \cdot 7 \cdot 3^2 \cdot 5^2 \cdot 7 = ab. \tag{4.45}$$

Lause 5

Olkoot $a, b \in \mathbb{Z}^+$, tällöin

$$ab = syt(a, b)pyj[a, b] = (a, b)[a, b]. \tag{4.46}$$

Todistus. Kotitehtävä.
Osoita ensin, että

$$\min(r_i, s_i) + \max(r_i, s_i) = r_i + s_i. \tag{4.47}$$

Lemma 3

Olkoot $a, b, c \in \mathbb{Z}$ ja merkitään $e = syt(a, b)$, $g = syt(b, c)$. Jos on olemassa $q \in \mathbb{Z}$ siten, että

$$a + qb + c = 0, \tag{4.48}$$

niin $e = g$.

Eukleideen algoritmi

Jakoalgoritmin nojalla saadaan/by the division algorithm we get
Eukleideen algoritmi= E.A. Olkoot $a, b \in \mathbb{Z}^+$ annettu ja $1 \leq b < a$:

$$
\begin{aligned}
& r_0 = a, \ r_1 = b && 0 \leq r_1 < r_0 \\
& r_0 = q_1 r_1 + r_2 && 0 \leq r_2 < r_1 \\
& \dots \\
& r_k = q_{k+1} r_{k+1} + r_{k+2} && 0 \leq r_{k+2} < r_{k+1} \\
& \dots \\
& r_{n-2} = q_{n-1} r_{n-1} + r_n && 0 \leq r_n < r_{n-1} \\
& \exists \ n \in \mathbb{N} : && r_n \neq 0, \ r_{n+1} = 0 \\
& r_{n-1} = q_n r_n \\
& r_n = \text{syt}(a, b).
\end{aligned}
$$

Here/Tässä $n =$ Eukleideen algoritmin pituus/length, which satisfies/ jolle pätee

$$n \leq a - 1. \tag{4.49}$$

Later we shall prove using Fibonacci numbers/myöhemmin todistetaan Fibonaccin lukujen avulla, että

$$n \leq \log a / \log((1 + \sqrt{5})/2)). \tag{4.50}$$

Set now/Asetetaan nyt

$$R_k = \begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix}, \; Q_k = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}, \; k \in \mathbb{N}, \tag{4.51}$$

whereupon/jolloin

$$\det Q_k = -1, \quad {Q_k}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix}. \tag{4.52}$$

We see that/Nähdään, että

$$\text{E.A.} \Leftrightarrow R_k = Q_{k+1} R_{k+1}, \; \forall k = 0, \ldots, n-1, \tag{4.53}$$

whereupon holds/jolloin pätee

$$R_0 = Q_1 Q_2 \cdots Q_k R_k. \tag{4.54}$$

Denote/Merkitään

$$S_0 = \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{4.55}$$

ja

$$S_k = \begin{pmatrix} s_k & t_k \\ s_{k+1} & t_{k+1} \end{pmatrix} = {Q_k}^{-1} \cdots {Q_2}^{-1} {Q_1}^{-1}, \tag{4.56}$$

jolloin

$$R_k = S_k R_0. \tag{4.57}$$

Nyt

$$S_{k+1} = Q_{k+1}^{-1} S_k \tag{4.58}$$

eli

$$\begin{pmatrix} s_{k+1} & t_{k+1} \\ s_{k+2} & t_{k+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{k+1} \end{pmatrix} \begin{pmatrix} s_k & t_k \\ s_{k+1} & t_{k+1} \end{pmatrix} =$$

$$\begin{pmatrix} s_{k+1} & t_{k+1} \\ s_k - q_{k+1} s_{k+1} & t_k - q_{k+1} t_{k+1} \end{pmatrix} \tag{4.59}$$

$\Leftrightarrow$ Palautuskaavat eli rekursiot/recurrences:

$$\begin{cases} s_{k+2} = s_k - q_{k+1} s_{k+1}, \ \ k = 0, 1, \ldots \\ t_{k+2} = t_k - q_{k+1} t_{k+1}, \ \ k = 0, 1, \ldots \end{cases} \tag{4.60}$$

From formula/Yhtälöstä (4.57) we get/saadaan

$$r_n = s_n a + t_n b, \tag{4.61}$$

josta edelleen/further saadaan

Lause 6

$$syt(a, b) = s_n a + t_n b, \tag{4.62}$$

where/missä n on E.A:n pituus/lenght.

Esimerkki 13

Olkoot $a = 909$ *ja* $b = 309$. *Tällöin Eukleideen algoritmilla saadaan*

$$q_1 = 2, \quad q_2 = 1, \quad q_3 = 16, \quad q_4 = 6, \quad r_4 = 3, \quad n = 4. \tag{4.63}$$

Next we use/Seuraavaksi käytetään rekursioita (4.60) starting from initial values/lähtien alkuarvoista (4.55). By calculating/Laskemalla saadaan

$$s_4 = 17, \quad t_4 = -50 \quad \Rightarrow \quad s_4 a + t_4 b = 3. \tag{4.64}$$

Seuraus 1

Olkoot $a, b, c \in \mathbb{Z}$. *Tällöin, if/jos*

$$a|bc \quad ja \quad a \perp c, \tag{4.65}$$

then/niin

$$a|b. \tag{4.66}$$

Todistus. Koska $a \perp c$, niin on olemassa sellaiset $s, t \in \mathbb{Z}$, että

$$1 = sa + tc \quad \Rightarrow \quad b = sab + tcb \quad \Rightarrow \quad a|b. \quad \square \tag{4.67}$$

Seuraus 2

Olkoot $a, b, c \in \mathbb{Z}$. *Tällöin, jos*

$$a|c \quad ja \quad b|c \quad ja \quad a \perp b, \tag{4.68}$$

niin

$$ab|c. \tag{4.69}$$

Proof. By the assumption $a|c$ there exists an $k \in \mathbb{Z}$ such that $c = ka$. By the assumption $b|c$ we get $b|ka$. By the assumption $a \perp b$ and Corollary 1 it follows $b|k$. Thus there exists an $l \in \mathbb{Z}$ such that $k = lb$. Hence $c = lba$ which implies $ab|c$. □

Seuraus 3

Olkoot $a, b \in \mathbb{Z}$ *ja* $p \in \mathbb{P}$. *Tällöin, jos*

$$p|ab, \tag{4.70}$$

niin

$$p|a \quad tai \quad p|b. \tag{4.71}$$

Todistus. Vastaoletus $p \not| a$ ja $p \not| b$. Tällöin $p \perp b$, joten oletuksen $p|ab$ ja Korollaarin 1 nojalla $p|a$. Ristiriita vastaoletuksen kanssa. □

Seuraus 4

Olkoot $a \in \mathbb{Z}$, $p \in \mathbb{P}$ *ja* $k, n \in \mathbb{Z}^+$. *Tällöin*

$$p|a^n \quad \Rightarrow \quad p|a \quad \Rightarrow \quad p^n|a^n; \tag{4.72}$$

$$p^k|a^n \quad \Rightarrow \quad p|a^n. \tag{4.73}$$

Määritelmä 13

Olkoot $a_1, ..., a_m \in \mathbb{Z}$ *be given/annettu. Tällöin luku* $d_m \in \mathbb{N}$ *on lukujen* $a_1, ..., a_m$ *suurin yhteinen tekijä eli*
$d_m = syt(a_1, ..., a_m) = gcd(a_1, ..., a_m) = (a_1, ..., a_m)$ *mikäli*

$$\begin{aligned} a) \quad & d_m | a_i \quad \forall i = 1, ..., m; \\ b) \quad & c | a_i \quad \forall i = 1, ..., m \quad \Rightarrow \quad c | d_m. \end{aligned}$$

Huomautus 3

Olkoot $a_1, ..., a_m \in \mathbb{Z}$ *pareittain keskenään jaottomia/ pairwise relatively prime eli*

$$a_i \perp a_j \quad \forall i \neq j. \tag{4.74}$$

Tällöin

$$(a_1, ..., a_m) = 1. \tag{4.75}$$

Huomautus 4

Not necessarily valid to the other direction/ Edellinen ei päde välttämättä vastakkaiseen suuntaan, because e.g./sillä esimerkiksi

$$(6, 9, 5) = 1 \quad \textit{mutta} \quad (6, 9) = 3. \tag{4.76}$$

Määritelmä 14

Olkoot $a_1, ..., a_m \in \mathbb{Z}$ *annettu. Tällöin luku* $f_m \in \mathbb{N}$ *on lukujen* $a_1, ..., a_m$ *pienin yhteinen jaettava/least common multiple eli*
$f_m = pyj[a_1, ..., a_m] = [a_1, ..., a_m]$ *mikäli*

$$\begin{aligned} a) \quad & a_i | f_m \quad \forall i = 1, ..., m; \\ b) \quad & a_i | c \quad \forall i = 1, ..., m \quad \Rightarrow \quad f_m | c. \end{aligned}$$

Lause 7

Olkoon $d_m = (a_1, ..., a_m)$*, tällöin on olemassa sellaiset/then there exist* $l_1, ..., l_m \in \mathbb{Z}$*, että/such that*

$$d_m = l_1 a_1 + ... + l_m a_m. \tag{4.77}$$

Todistus: Induktiolla.
Base case/Perusaskel: $m = 2 \Leftrightarrow$ (4.62).
Induction hypothesis/Induktio-oletus: Claim is valid when/Väite tosi, kun $m = k$.
Induktioaskel/Induction step: Olkoon $m = k + 1$.

1. First we show, that/Osoitetaan ensin, että

$$d_{k+1} = (d_k, a_{k+1}). \tag{4.78}$$

a.) Because/Koska

$$d_{k+1} | a_1, ..., a_k, a_{k+1}, \tag{4.79}$$

niin

$$d_{k+1} | d_k, \quad d_{k+1} | a_{k+1} \tag{4.80}$$

eli on yhteinen tekijä/is a common factor.

b.) Jos

$$c|d_k,\ \ a_{k+1}, \tag{4.81}$$

niin

$$c|a_1, ..., a_k, a_{k+1}. \tag{4.82}$$

Siten

$$c|d_{k+1}, \tag{4.83}$$

joten on suurin tekijä/is the largest factor. a.)+b.)$\Rightarrow$ $d_{k+1} = (d_k, a_{k+1})$.

2. Induktio-oletuksesta saadaan, että/from the induction hypothesis we get

$$\exists \quad h_i \in \mathbb{Z}: \quad d_k = h_1 a_1 + ... + h_k a_k \tag{4.84}$$

ja

$$\exists \quad j_i \in \mathbb{Z}: \quad (d_k, a_{k+1}) = j_1 d_k + j_2 a_{k+1}. \tag{4.85}$$

Thus/Siten

$$d_{k+1} = (d_k, a_{k+1}) =$$

$$j_1(h_1 a_1 + ... + h_k a_k) + j_2 a_{k+1} = l_1 a_1 + ... + l_{k+1} a_{k+1}. \tag{4.86}$$

Joten induktioaskel on todistettu ja induktioperiaatteen nojalla alkuperäinen lauseen väite on tosi. Hence the induction step is proved and by the induction principle the original claim of the theorem is proved. □

Tämänkin luvun käsitteet ja tulokset ovat suurelta osin peruskursseilta, joten todistukset annetaan vain valikoiduista tuloksista.

Esimerkki 14

Huomataan, että

$$17 = 3 \cdot 5 + 2, \quad 12 = 2 \cdot 5 + 2, \quad 7 = 1 \cdot 5 + 2, ..., \tag{5.1}$$

jolloin on sovittu merkinnästä

$$17 \equiv 2 \pmod 5, \quad 12 \equiv 7 \equiv 2 \pmod 5. \tag{5.2}$$

Määritelmä 15

Olkoon $n \in \mathbb{Z}^+$ *annettu/given ja* $a, b \in \mathbb{Z}$. *Jos/If*

$$n|a - b, \tag{5.3}$$

niin tällöin asetetaan/then we set

$$a \equiv b \pmod{n} \tag{5.4}$$

eli a on kongruentti b:n kanssa modulo n/a is congruent to b modulo n. Edelleen/Further, luku n on kongruenssin (5.4) modulus. Merkitään/Let us denote

$$a \not\equiv b \pmod{n}, \tag{5.5}$$

kun a ei ole kongruentti b:n kanssa modulo n/when is not.

Huomautus 5

Työkaluja:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad a - b \equiv 0 \pmod{n}; \tag{5.6}$$

$$a \equiv 0 \pmod{n} \quad \Leftrightarrow \quad n \mid a. \tag{5.7}$$

Lause 8

Kongruenssi on ekvivalenssirelaatio.
Olkoon $n \in \mathbb{Z}^+$, $a, b, c \in \mathbb{Z}$. *Tällöin pätee*

$$a \equiv a; \tag{5.8}$$

$$a \equiv b \quad \Leftrightarrow \quad b \equiv a; \tag{5.9}$$

$$a \equiv b, \ b \equiv c \quad \Rightarrow \quad a \equiv c; \tag{5.10}$$

kaikki kongruenssit $\pmod{n}$.

Lause 9

Kongruenssin laskusääntöjä.
Olkoon $n \in \mathbb{Z}^+$, $a, b, c, d, r, s \in \mathbb{Z}$, $h \in \mathbb{N}$ ja $P(x) \in \mathbb{Z}[x]$. Jos

$$a \equiv b, \ c \equiv d, \tag{5.11}$$

niin

$$ra + sc \equiv rb + sd; \tag{5.12}$$

$$a \pm c \equiv b \pm d; \tag{5.13}$$

$$ac \equiv bd; \tag{5.14}$$

$$a^h \equiv b^h; \tag{5.15}$$

$$P(a) \equiv P(b); \tag{5.16}$$

kaikki kongruenssit $\pmod{n}$.

Todistus. Käytetään työkaluja (5.6) ja (5.7) sekä jaollisuuden laskusääntöjä.
Kohta (5.12): Oletuksista (5.11) seuraa

$$n|a-b, \quad n|c-d \quad \Rightarrow \tag{5.17}$$

$$ra+sc-(rb+sd)=r(a-b)+s(c-d)\equiv 0 \pmod{n}, \tag{5.18}$$

jolloin tuloksen (5.6) nojalla saadaan väite. □

Esimerkki 15

$$a \equiv a+ln \pmod{n} \quad \forall l \in \mathbb{Z}. \tag{5.19}$$

Muita tuloksia

Lause 10

Olkoon $n \in \mathbb{Z}^+$, $a, b, m \in \mathbb{Z}$, $m \neq 0$. *Tällöin pätee*

A.

$$ma \equiv mb \pmod{n}, \quad m \perp n \quad \Rightarrow \tag{5.20}$$

$$a \equiv b \pmod{n}. \tag{5.21}$$

B.

$$a \equiv b \pmod{mn}, \quad m \in \mathbb{Z}^+, \quad \Rightarrow \tag{5.22}$$

$$a \equiv b \pmod{n}. \tag{5.23}$$

Proof. Case A. From the assumptions (5.20) follows that there exists a $k \in \mathbb{Z}$ such that

$$ma = mb + kn, \quad \Rightarrow \quad m|kn. \tag{5.24}$$

But $m \perp n$ forcing $m|k = hm$, $h \in \mathbb{Z}$, which implies

$$ma = mb + hmn, \quad \Rightarrow \quad a = b + hn \quad \Rightarrow \quad a \equiv b \pmod{n}. \quad \square \tag{5.25}$$

Huomautus 6

$$a \equiv b \pmod{n} \quad \Leftrightarrow \tag{5.26}$$

$$n \mid a - b \Leftrightarrow a = b + l \cdot n, \ \textit{jollakin } l \in \mathbb{Z} \tag{5.27}$$

$$\Leftrightarrow a \in b + n\mathbb{Z} = \overline{b}, \tag{5.28}$$

missä $\overline{b}$ *on edustajan* b *määräämä jakojäännösluokka* $\pmod{n}$*./* $\overline{b}$ *is the residue/congruence class* $\pmod{n}$ *determined by the representative* b*.*

Lause 11

A. Keskenään kongruenteilla luvuilla on samat jakojäännökset ja Vice Versa.

B. Kongruentit luvut kuuluvat samaan jakojäännösluokkaan eli

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad \overline{a} = \overline{b}. \tag{5.29}$$

Siispä joukkoa

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a}|a = 0, 1, 2, \ldots, n-1\} = \mathbb{Z}_n \tag{5.30}$$

kutsutaan jakojäännösrenkaaksi, missä on laskutoimitukset/residue class ring with binary operations

$$\overline{a} + \overline{b} = \overline{a+b}, \tag{5.31}$$

$$\overline{a}\overline{b} = \overline{ab}. \tag{5.32}$$

Huomautus 7

Jakojäännösluokalle $\overline{b}$ voidaan käyttää myös merkintää $[b]$ (Ryhmäteoreettinen sivuluokka/Group theoretic coset).

Huomautus 8

Usein kuitenkin lasketaan vain pelkillä edustajilla eli jakojäännöksillä $0, 1, 2, ..., n-1 = -1 \pmod{n}$*./ Often we use just the remainders.*

Esimerkki 16

$$-1+1 = n-1+1 = n = 0, \quad (-1)^{-1} = -1 \pmod{n}, \tag{5.33}$$

$$2^{-1} = \frac{1}{2} = \frac{p+1}{2} \pmod{p}, \quad p \in \mathbb{P}_{p \geq 3}. \tag{5.34}$$

Määritelmä 16

Olkoon R ykkösellinen rengas. Joukko

$$R^* = \{\textit{yksiköt}\} = \{u \in R \mid \exists\ u^{-1} \in R :\ uu^{-1} = 1\} \tag{5.35}$$

on renkaan R yksikköryhmä/unit group of the ring.

Esimerkki 17

Jos $R = K$-kunta, niin

$$K^* = K\backslash\{0\}. \tag{5.36}$$

$$\mathbb{Z}^* = \{\pm 1\}. \tag{5.37}$$

Lause 12

Joukko

$$\{\overline{a} \in \mathbb{Z}_n | \ a \perp n\}$$

on renkaan $\mathbb{Z}_n$ *yksikköryhmä eli*

$$\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n | \ a \perp n\}. \tag{5.38}$$

Huomaa,että ehdosta/Note that from the condition $a \perp n$ seuraa Eukleideen algoritmin seurauksen (4.62) nojalla, että

$$1 = s_m a + t_m n, \tag{5.39}$$

missä m on E.A:n pituus. Siten

$$s_m a \equiv 1 \pmod{n} \Leftrightarrow \overline{a}^{-1} = \overline{s_m}. \tag{5.40}$$

Erityisesti/In particular, jos $p \in \mathbb{P}$, niin $\mathbb{Z}_p$ on kunta ja

$$\mathbb{Z}_p^* = \{\overline{a} \in \mathbb{Z}_p | \ a \perp p\} = \{\overline{1}, \overline{2}, ..., \overline{p-1}\}. \tag{5.41}$$

Määritelmä 17

Olkoon $n \geq 2$. Jos $a \perp n$, niin $\overline{a}$ on alkuluokka (mod n) ja

$$\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n | \ a \perp n\}$$

on renkaan $\mathbb{Z}_n$ kertolaskuryhmä (multiplication group of the ring).

Määritelmä 18

Eulerin funktio $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ saadaan asettamalla

$$\varphi(n) = \#\{k \in \mathbb{Z}^+ \mid 1 \leq k \leq n, \ k \perp n\} \tag{5.42}$$

aina, kun $n \in \mathbb{Z}^+$.

Siten, ryhmän $\mathbb{Z}_n^*$ kertaluku (order) on

$$\#\mathbb{Z}_n^* = \varphi(n), \quad n \in \mathbb{Z}_{\geq 2}. \tag{5.43}$$

Lemma 4

Eulerin funktio φ on multiplikatiivinen eli

$$\varphi(MN) = \varphi(M)\varphi(N), \ \forall M \perp N. \tag{5.44}$$

Olkoon $p \in \mathbb{P}$, $m \in \mathbb{Z}^+$, tällöin

$$\varphi(p^m) = p^m \left(1 - \frac{1}{p}\right). \tag{5.45}$$

Seurauksena saadaan laskukaava

Lause 13

Olkoon $n = p_1^{a_1} \dots p_k^{a_k}$, $p_i \in \mathbb{P}$. Tällöin

$$\varphi(n) = {p_1}^{a_1} \dots {p_k}^{a_k} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right) \tag{5.46}$$

eli

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right). \tag{5.47}$$

Tulo kaikkien n:n erillisten alkutekijöiden yli. Product over all distinct prime factors of n.

Euler-Fermat theorem/Fermat'n pieni lause

Lause 14

Olkoot $a \in \mathbb{Z}$, $n \in \mathbb{Z}_{\geq 2}$ annettu ja $a \perp n$. Tällöin

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \tag{5.48}$$

Lause 15

FERMAT'N PIKKULAUSE: Olkoon $p \in \mathbb{P}$ annettu. Tällöin

$$a^{p-1} \equiv 1 \pmod{p}, \quad \textit{jos} \quad p \nmid a \in \mathbb{Z}; \tag{5.49}$$

$$a^{p} \equiv a \pmod{p}, \quad \forall\ a \in \mathbb{Z}. \tag{5.50}$$

Olettaen (5.49) todistetaan (5.50):
Jos syt$(a, p) = 1$, niin Pikku Fermat'n (5.49) nojalla

$$a^p \equiv a \pmod{p}. \tag{5.51}$$

Jos $p|a$, niin

$$a \equiv 0 \pmod{p} \quad \Rightarrow \quad a^p \equiv 0 \pmod{p} \tag{5.52}$$

$$\Rightarrow \quad a^p \equiv a \pmod{p}. \quad \square \tag{5.53}$$

A congruence system

Lause 16

A) Olkoot $p, q \in \mathbb{P}$ ja $p \neq q$. Tällöin yhtälöistä

$$\begin{cases} a \equiv b \pmod{p} \\ a \equiv b \pmod{q} \end{cases} \tag{5.54}$$

seuraa

$$a \equiv b \pmod{pq}. \tag{5.55}$$

B) Let $m_i \in \mathbb{Z}$ ja $m_i \perp m_j$ for all $i \neq j$. Then from the equations

$$a \equiv b \pmod{m_i} \quad \forall \quad i = 1, ..., r \tag{5.56}$$

follows

$$a \equiv b \pmod{m_1 \cdots m_r}. \tag{5.57}$$

Todistus. A) kohta: Oletuksista (5.54) seuraa/From the assumptions follows

$$p|a-b, \quad q|a-b. \tag{5.58}$$

Koska/Because $p \perp q$, niin Seurauksen 2 nojalla/by

$$pq|a-b \quad \Leftrightarrow \quad a \equiv b \pmod{pq}. \quad \square \tag{5.59}$$

B) kohta induktiolla.

Esimerkki 18

Olkoot $p, q \in \mathbb{P}$ ja $p \neq q$. Tällöin

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}. \tag{5.60}$$

Todistus. Lasketaan ensin erilliset kongruenssit/First we compute the separate congruences

$$p^{q-1} + q^{p-1} \equiv 0 + 1 = 1 \pmod{p}; \tag{5.61}$$

$$p^{q-1} + q^{p-1} \equiv 1 + 0 = 1 \pmod{q}. \tag{5.62}$$

$$\tag{5.63}$$

Soveltamalla Lausetta 16 kohta A, saadaan väite (5.60)./ By applying Theorem 16 case A, we get the claim (5.60).

Kiinalainen jäännöslause/Chinese remainder theorem

Lause 17

Olkoot $m_1, \ldots, m_r \in \mathbb{Z}^+$ pareittain keskenään jaottomia ja olkoot $a_1, \ldots, a_r \in \mathbb{Z}$ annettu. Tällöin yhtälöryhmän

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases} \tag{5.64}$$

ratkaisut ovat

$$x = x_0 + l \cdot M, \; l \in \mathbb{Z}, \quad M = m_1 \ldots m_r = m_k M_k, \tag{5.65}$$

missä

$$x_0 = n_1 M_1 a_1 + \ldots + n_r M_r a_r, \tag{5.66}$$

$$n_k M_k \equiv 1 \pmod{m_k}. \tag{5.67}$$

Todistus: Aluksi huomataan, että/First we note

$$M_k \perp m_k, \tag{5.68}$$

sillä, jos olisi/if it were

$$1 < d = (M_k, m_k) \quad \Rightarrow \quad \exists\, p \in \mathbb{P} : \; p|d \quad \Rightarrow \tag{5.69}$$

$$p|m_k, \quad p|M_k = \prod_{i \neq k} m_i \quad \Rightarrow \quad p|m_i, \; i \neq k \quad \Rightarrow \tag{5.70}$$

$$p|(m_k, m_i) \quad \text{Ristiriita.} \tag{5.71}$$

Niinpä/Thus

$$\overline{M_k} \in \mathbb{Z}_{m_k}^* \quad \Rightarrow \quad \exists\, \overline{M_k}^{-1} := \overline{n_k} \in \mathbb{Z}_{m_k}^* \tag{5.72}$$

$$\Leftrightarrow \quad \overline{n_k}\overline{M_k} = \overline{1} \in \mathbb{Z}_{m_k}^* \tag{5.73}$$

$$\Leftrightarrow \quad n_k M_k \equiv 1 \pmod{m_k}. \tag{5.74}$$

Seuraavaksi huomataan, että/Next we note

$$M_j = \prod_{i \neq j} m_i \equiv 0 \pmod{m_k} \quad \forall j \neq k, \tag{5.75}$$

joten laskemalla saadaan/therefore by computing

$$x_0 = n_1 M_1 a_1 + \ldots + n_r M_r a_r \equiv \tag{5.76}$$

$$n_k M_k a_k \equiv 1 \cdot a_k = a_k \pmod{m_k} \quad \forall k = 1, ..., r \tag{5.77}$$

ja siten x_0 on eräs ratkaisu/is a solution.
Olkoon x ratkaisu, tällöin

$$x - x_0 \equiv 0 \pmod{m_k} \quad \forall k = 1, ..., r. \tag{5.78}$$

Koska $m_i \perp m_j \; \forall i \neq j$, niin Lauseen 16 kohdan B) nojalla

$$x - x_0 \equiv 0 \pmod{m_1 \cdots m_r} \tag{5.79}$$

eli

$$x \equiv x_0 \pmod{M}. \quad \square \tag{5.80}$$

Esimerkki 19

Solve

$$\begin{cases} x \equiv 1 \pmod 3, \\ x \equiv 2 \pmod 4, \\ x \equiv 3 \pmod 5. \end{cases} \tag{5.81}$$

Here $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, which are pairwise relatively prime. Thus $M_1 = 20$, $M_2 = 15$, $M_3 = 12$. Next we compute inverses of them

$$n_1 M_1 \equiv 1 \pmod{m_1} \Leftrightarrow \quad n_1 2 \equiv 1 \pmod 3 : \quad n_1 = 2; \tag{5.82}$$

$$n_2 M_2 \equiv 1 \pmod{m_2} \Leftrightarrow \quad n_2 3 \equiv 1 \pmod 4 : \quad n_2 = 3; \tag{5.83}$$

$$n_3 M_3 \equiv 1 \pmod{m_3} \Leftrightarrow \quad n_3 2 \equiv 1 \pmod 5 : \quad n_3 = 3. \tag{5.84}$$

Hence, the general solution is given by

$$x = n_1 M_1 a_1 + n_2 M_2 a_2 + n_3 M_3 a_3 + l \cdot M = 238 + l \cdot 60, \quad l \in \mathbb{Z}. \tag{5.85}$$

E.g.

$$238, 178, 118, 58, -2 \tag{5.86}$$

are solutions. Further, the general solution may be given e.g. by

$$x = -2 + k \cdot 60, \quad k \in \mathbb{Z}. \tag{5.87}$$

CHECK!

Esimerkki 20

Kotitehtävä 9. Olkoot $a, m, n \in \mathbb{Z},\ a \geq 2, m, n \geq 1$. Osoita, että

$$\text{syt}(a^m - 1,\ a^n - 1) = a^{\text{syt}(m,n)} - 1. \tag{5.88}$$

Ratkaisu: Merkitään $d :=\text{syt}(m, n)$, $m = ed$, $n = fd$, jolloin $e \perp f$ ja siten on olemassa sellaiset $s, t \in \mathbb{Z}$, että

$$1 = se + tf. \tag{5.89}$$

Merkitään vielä $D := a^d - 1$, jolloin väite (5.88) on muotoa

$$\text{syt}(a^m - 1,\ a^n - 1) = D. \tag{5.90}$$

[C.D] Yhteinen tekijä? Nyt

$$a^d \equiv 1 \pmod{D} \quad \Rightarrow \quad \begin{cases} a^m - 1 = (a^d)^e - 1 \equiv 0 \pmod{D}; \\ a^n - 1 = (a^d)^f - 1 \equiv 0 \pmod{D} \end{cases} \tag{5.91}$$

eli

$$\begin{cases} D | a^m - 1; \\ D | a^n - 1. \quad OK. \end{cases} \tag{5.92}$$

[G.] Suurin tekijä? Merkitään hetkeksi $A := a^d$. Olkoon C yhteinen tekijä eli

$$\begin{cases} C|a^m - 1; \\ C|a^n - 1. \end{cases} \Rightarrow \begin{cases} A^e = (a^d)^e = a^m \equiv 1 \pmod{C}; \\ A^f = (a^d)^f = a^n \equiv 1 \pmod{C}. \end{cases} \tag{5.93}$$

Niinpä tosiasian (5.89) nojalla

$$A^1 = A^{se+tf} = (A^e)^s (A^f)^t \equiv 1 \pmod{C} \quad \Rightarrow$$
$$a^d \equiv 1 \pmod{C} \quad \Rightarrow \quad C|D. \quad OK. \quad \square \tag{5.94}$$

Esimerkki 21

Homework 6a. Investigate for which numbers $n \in \mathbb{Z}_{\geq 1}$ holds

$$n^2 + 1 \in \mathbb{P}\,? \tag{5.95}$$

This is an open problem in general but we may do something.

1. Let $n = 1$, then $n^2 + 1 = 2 \in \mathbb{P}$.
2. Let $n = 2k + 1$, $k \in \mathbb{Z}_{\geq 1}$. Then

$$n^2 + 1 = 2(2k^2 + 2k + 1), \quad 2k^2 + 2k + 1 \geq 5. \tag{5.96}$$

3. Let $n = 2k$, $k \in \mathbb{Z}_{\geq 1}$. Then a numerical evidence

$$n^2 + 1 = 5,\ 17,\ 37,\ 65, \ldots \tag{5.97}$$

shows that the values are primes and composite numbers.
Let us show that

$$5 | n^2 + 1, \quad \forall\ n = \begin{cases} 2 + \ell \cdot 10; \\ 8 + \ell \cdot 10, \end{cases} \quad \ell \in \mathbb{Z}_{\geq 1}. \tag{5.98}$$

First we observe that

$$a^2 + 1 \equiv 0 \pmod 5 \qquad \forall\ a \equiv \begin{cases} 2 \\ 3 \end{cases} \pmod 5. \tag{5.99}$$

Applying to even n's this means that for

$$n \equiv \begin{cases} 2; \\ 8, \end{cases} \pmod{10} \tag{5.100}$$

we get

$$n^2 + 1 \equiv 0 \pmod{5}. \quad \square \tag{5.101}$$

Hence there are infinitely many composite numbers in the sequence $(n^2 + 1)$.
An old hypothesis claims that there are infinitely many primes in the sequence $(n^2 + 1)$.