Kongruenssi

$a \equiv b(\mathrm{mod}\, n) \Leftrightarrow$ Luvuilla a ja b on sama jakojäännös, kun ne jaetaan luvulla n.

$a \equiv b(\mathrm{mod}\, n) \Leftrightarrow n \mid (a-b)$
$a \equiv b(\mathrm{mod}\, n) \Leftrightarrow a = kn + b$

Kongruenssilla on seuraavat perusominaisuudet.
1° $a \equiv a(\mathrm{mod}\, n)$
2° Jos $a \equiv b(\mathrm{mod}\, n)$, niin $b \equiv a(\mathrm{mod}\, n)$
3° Jos $a \equiv b(\mathrm{mod}\, n)$ ja $b \equiv c(\mathrm{mod}\, n)$, niin $a \equiv c(\mathrm{mod}\, n)$

Kongruenssien laskusäännöt

1° Kongruenssit voidaan laskea puolittain yhteen ja vähentää puolittain.

$$+\begin{cases} a \equiv b(\mathrm{mod}\, n) \\ c \equiv d(\mathrm{mod}\, n) \end{cases} \qquad -\begin{cases} a \equiv b(\mathrm{mod}\, n) \\ c \equiv d(\mathrm{mod}\, n) \end{cases}$$
$$a + c \equiv b + d(\mathrm{mod}\, n) \qquad a - c \equiv b - d(\mathrm{mod}\, n)$$

2° Kongruenssit voidaan kertoa puolittain keskenään.

$$\cdot\begin{cases} a \equiv b(\mathrm{mod}\, n) \\ c \equiv d(\mathrm{mod}\, n) \end{cases}$$
$$ac \equiv bd(\mathrm{mod}\, n)$$

3° Kongruenssin molemmille puolille voidaan lisätä ja vähentää sama luku.

$$a \equiv b(\mathrm{mod}\, n) \quad \mid \pm k$$
$$a \pm k \equiv b \pm k(\mathrm{mod}\, n)$$

Jäännösluokka modulo n

$[m]_n = \underline{m} = \{x \in \mathbb{Z} \mid x \equiv m(\mathrm{mod}\, n)\}$

Jäännösluokilla modulo n on seuraavat ominaisuudet.
1° Jokainen kokonaisluku kuuluu vain yhteen jäännösluokkaan modulo n.
2° $[a] = [b]$ jos ja vain jos $a \equiv b(\mathrm{mod}\, n)$.
3° Jäännösluokkia on n kappaletta.

Jäännösluokista modulo n muodostuvaa joukkoa merkitään $\mathbb{Z}_n$.

Jäännösluokkien yhteen- ja kertolasku voidaan suorittaa seuraavasti.
$[a] + [b] = [a + b]$
$[a] \cdot [b] = [a \cdot b]$

Fermat'n pieni lause:
Olkoot a ja p keskenään jaottomia lukuja, joista a on kokonaisluku ja p on alkuluku. Tällöin $a^{p-1} \equiv 1(\mathrm{mod}\, p)$.

Alkuluvut <1000

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
293	307	311	313	317	331	337	347	349	353
359	367	373	379	383	389	397	401	409	419
421	431	433	439	443	449	457	461	463	467
487	491	499	503	509	521	523	541	547	557
563	569	571	577	587	593	599	601	613	617
619	631	641	647	653	659	661	673	677	683
691	701	709	719	727	733	743	751	757	761
769	773	787	797	809	811	821	823	827	829
839	853	857	859	863	877	881	883	887	907
911	919	929	937	941	947	953	967	971	977
983	991	997							