Kvaak'n kvaak kvaak

Heikki Pitkänen

4. joulukuuta 2013

Kvaak

Kvaak kvaak kvaak Kvaak'n kvaak kvaak, Kvaak kvaak kvaak kvaak kvaak. Kvaak p kvaak kvaak kvaak p kvaak a, kvaak $a^{p-1} \equiv 1 \pmod{p}$. Kvaak kvaak, kvaak kvaak kvaak kvaak, kvaak kvaak Kvaak'n kvaak kvaak kvaak kvaak kvaak. Kvaak kvaak Kvaak'n kvaak kvaak kvaak. Kvaak kvaak kvaak Kvaak kvaak Kvaak'n kvaak kvaak kvaak. Kvaak kvaak, kvaak kvaak kvaak kvaak kvaak kvaak kvaak kvaak.

1. Kvaak'n kvaak kvaak

Kvaak 1.1. Kvaak $p > 1$ kvaak *kvaak*, kvaak kvaak kvaak kvaak kvaak kvaak 1 kvaak kvaak kvaak p.

Kvaak 1.2. Kvaak kvaak $\equiv \pmod{p}$ kvaak

$$a \equiv b \pmod{p} \iff b = kp + a \text{ kvaak } k \in \mathbb{Z}.$$

Kvaak 1.3. Kvaak $\equiv \pmod{p}$ kvaak *kvaak* $\mathbb{Z}/_{\equiv \pmod{p}}$ kvaak

$$\mathbb{Z}_p := \{[0]_p, [1]_p, \ldots, [p-1]_p\}.$$

Kvaak 1.4. Kvaak $[a]_p \in \mathbb{Z}_p$ kvaak kvaak kvaak kvaak b, kvaak kvaak kvaak kvaak a kvaak kvaak p.

Kvaak 1.5. Kvaak kvaak $[a]$, kvaak kvaak $[a]_p$ kvaak p kvaak kvaak kvaak.

Kvaak 1.6. a) $21 \equiv 16 \equiv 1 \pmod{5}$, kvaak $16 = 3 \cdot 5 + 1$ kvaak $21 = 4 \cdot 5 + 1$
b) $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$
c) Kvaak $[3] \in \mathbb{Z}_5$. Kvaak $-7, -2, 3, 8, 13, \ldots \in [3]$

Kvaak 1.7. *Kvaak "$\cdot$" kvaak "$+$" kvaak kvaak kvaak* $\equiv \pmod{p}$ *kvaak.*

Kvaak. Kvaak $a \equiv a' \pmod{p}$ kvaak $b \equiv b' \pmod{p}$. Kvaak kvaak kvaak $r, s \in \mathbb{Z}$ kvaak, kvaak $a + rp = a'$ kvaak $b + sp = b'$. Kvaak kvaak $a' \cdot b'$.

$$\begin{aligned} a' \cdot b' &= (a + rp)(b + sp) \\ &= ab + asp + brp + srp^2 \\ &\equiv a \cdot b \pmod{p} \end{aligned}$$

Kvaak $a' \cdot b' \equiv a \cdot b \pmod{p}$. Kvaak "$\cdot$" kvaak kvaak kvaak. Kvaak kvaak $a' + b'$.

$$\begin{aligned} a' + b' &= (a + rp) + (b + sp) \\ &= a + b + (r + s)p \\ &\equiv a + b \pmod{p} \end{aligned}$$

Kvaak $a' + b' \equiv a + b \pmod{p}$. Kvaak kvaak "$+$" kvaak kvaak. □

Kvaak Kvaak'n kvaak kvaak kvaak kvaak kvaak kvaak kvaak kvaak kvaak kvaak kvaak kvaak kvaak kvaak kvaak kvaak.

Kvaak 1.8. Kvaak kvaak kvaak G kvaak e. Kvaak kvaak $a \in G$ *kvaak* kvaak kvaak kvaak kvaak k, kvaak $a^k = e$ kvaak kvaak $\#a = k$. Kvaak G *kvaak* kvaak kvaak kvaak kvaak kvaak kvaak $\#G$.

Kvaak 1.9. Kvaak G kvaak *kvaak*, kvaak kvaak kvaak $a \in G$ kvaak, kvaak

$$G = \{a^k : k \in \mathbb{N}\} =: \langle a \rangle.$$

Kvaak, kvaak kvaak *a kvaak kvaak* G.

Kvaak 1.10 (Kvaak kvaak)**.** *Kvaak* G *kvaak kvaak, kvaak kvaak* $H \subset G$ *kvaak* G *kvaak. Kvaak*

$$\#G = \#(G/H)\#H = \#(H\backslash G)\#H.$$

Kvaak $\#G = k\#H$ *kvaak* $k \in \mathbb{N}$.

Kvaak 1.11. Kvaak kvaak $a, b \in \mathbb{N}$ *kvaak kvaak kvaak* k kvaak kvaak kvaak kvaak, kvaak kvaak kvaak a kvaak b, kvaak $k \mid a$ kvaak $k \mid b$. Kvaak kvaak $\operatorname{syt}(a, b) = k$.

Kvaak 1.12. *Kvaak* $\operatorname{syt}(a, p) = d$*, kvaak* $ax \equiv d \pmod{p}$ *kvaak kvaak.*

Kvaak. Kvaak $\operatorname{syt}(a, p) = d$, kvaak kvaak $r, s \in \mathbb{Z}$ kvaak kvaak Kvaak'n kvaak $ar + ps = d$. Kvaak $ar = -ps + d$ kvaak kvaak $ar \equiv d \pmod{p}$. Kvaak kvaak kvaak kvaak r. □

Kvaak 1.13 (Kvaak'n kvaak)**.** *Kvaak* p *kvaak kvaak kvaak kvaak* $p \nmid a$ *kvaak* $a^{p-1} \equiv 1 \pmod{p}$.

Kvaak. Kvaak p kvaak kvaak kvaak $p \nmid a$ kvaak $a \not\equiv 0 \pmod{p}$. Kvaak kvaak kvaak kvaak $\mathbb{Z}_p^* = \{[a] \in \mathbb{Z}_p : p \nmid a\} = \{[1], [2], \ldots, [p-1]\}$ kvaak kvaak kvaak kvaak.

Kvaak kvaak kvaak kvaak, kvaak $[1]$. Kvaak kvaak kvaak kvaak kvaak $[a] \in Z_p^*$. Kvaak p kvaak kvaak, kvaak $\operatorname{syt}(a, p) = 1$ kvaak kvaak $ax \equiv 1 \pmod{p}$ kvaak kvaak 1.12 kvaak kvaak x, kvaak $[a]^{-1} = [x]$ kvaak kvaak $[a]$ kvaak.

Kvaak $\mathbb{Z}_p^*$ kvaak $[a]$ kvaak kvaak kvaak $\langle [a] \rangle$ kvaak kvaak $\mathbb{Z}_p^*$ kvaak. Kvaak Kvaak kvaak kvaak $\#\langle [a] \rangle \mid p - 1$ kvaak kvaak $k \in \mathbb{Z}$ kvaak $p - 1 = k\#\langle [a] \rangle$. Kvaak kvaak kvaak kvaak kvaak $[a]^{\#\langle [a] \rangle} = 1$, kvaak kvaak

$$[a^{p-1}] = [a]^{p-1} = [a]^{k\#\langle [a] \rangle} = [1]^k = [1]$$

Kvaak $a^{p-1} \equiv 1 \pmod{p}$.

□

Kvaak 1.14. *Kvaak* p *kvaak kvaak, kvaak* $a^p \equiv a \pmod{p}$.

Kvaak. Kvaak $p \nmid a$, kvaak Kvaak'n kvaak kvaak $a^{p-1} \equiv 1 \pmod{p}$, kvaak kvaak kvaak kvaak kvaak a kvaak kvaak. Kvaak $p \mid a$, kvaak $p \mid a^p$, kvaak kvaak $a \equiv 0 \pmod{p}$, kvaak $a^p \equiv 0 \pmod{p}$. □

Kvaak 1.15. Kvaak 3 kvaak 5 kvaak kvaak, kvaak

a) $2^3 = 8 \equiv 2 \pmod{3}$
b) $4^5 = 1024 \equiv 4 \pmod{5}$.

Kvaak

[1] Kvaak, K. K. & Kvaak, K. K.: *Kvaak kvaak kvaak kvaak kvaak kvaak kvaak,* Kvaak kvaak kvaak, Kvaak 2008.

[2] Kvaak, Kvaak K. & K. Kvaak: *Kvaak kvaak kvaak,* Kvaak-Kvaak, Kvaak 2005.

[3] Kvaak. K: *Kvaak kvaak kvaak: kvaak kvaak,* `http://isotropic.org/papers/chicken.pdf`, kvaak 4.12.2013.