Wycliffe ASSOCIATES

Our Daily Bread Ministries®

ourdailybread.org

✓ ㄱ

ㄴ 🕮 : 🐡 ㅆ ㅅ : ㅙ → ㅙㅅ

ㄱㄴ 🕮 : " ㅛ = ㅎ ㅇ . ㅎ →ㅇ ㅇ △ ㅌ . ㅇ ✕ ㅇ→ ㄱ . ㅇ ㅇ→ ㅎ . " ㅠ ㅆ ㅅ : ㅅㅅ

ㅎ ㅗ ㅛ ㅎ .

ㅜ ㅅㅅ ㅎ ✓ ㄱ . ㅎ ㅈ . ㅌ ㅁ ㅎ ♡ ♡ . ㅎ ㅍ ㅎ . ㅎ ㅗ 초 ㅁ ㅆ . ㅎ ✓ ㄱ . ㅎ ∨ ✓ ㅅㅅ . ㅎ ✓ ㄱ .

ㅎ ㅗ ✓ △△ . ㅌ ㅁ △△ ✕ // → ㅎ . 🕮 ㅁ ✕ 人 ㅆ . ㅎ ㅗ ✓ △△ . ㅎ ㅗ ✕ = ✓ ㅎ 🕮 . ㅎ ㅇ ㅗ ㅎ = ㅆ . ✓ ㅈ ✕ ㅎ ㅎ ㅿ ㅆ . ㅎ ㅇ ㅇ ㅜ . ㅜ ㅈ ㅇ→ ㅎ . ㅎ ㅌ ㅜ . ㅌ ㅜ // → ㅎ .

ㅆ ㅅ ㅇ ㅎ ㅈ . ㅜ ㅈ ㅅ ㅌ ? ㅎ . ㅎ ✕ ✓ . ㅎ ㅇ ㅌ

ㅜ . ㅎ = ㅎ ㅇ . ㅎ ✕ ㅗ ㅇ . ㅎ ㅇ ∨ ㅊ .

ㅈㅎ

ㄴ 🕮 : 🐷 ㅙㅙ : ㅙㅙ → ㅆㅙ

ㄱㄴ 🕮 : " ㅋ 괴 ㅁ ㅿㅿ ㅛ ㅒ ㅅ . " 🐷 ㅙ ㅆ : ㅙ

ㅎ ㅗ ㅎ ㅇ . ㅎ ㅇ ㅎ ♡ .

ㅊ ㅇㅇ ㅋ 目 // . ㅋ ㄱㅈ △ . ㅊ ㅇㅇ ㅋ ㅛ ㄱ 괴 ㄴ . ㅊ ㅇ ㅇ ㅋ ㅇ . ㅙ ㅇ ㅋ 目 ㄱ ㅿ // . ㄱ ㅙ . ㅜ ㄱ ? ㅋ ✕ ㅁ . ㅋ 目 ㄱ ㅈ . ㅇ! ㄱ ㅜ ㄱ .

ㄱ ㅂ ㅿ ㅿ ㅋ 目 ㄱ . ㅋ ♡ ㄱ . ㅋ ㅈ → ㄱ . ㅋ 犬 犬 ㅿ ㄱ . ㅋ □ㅇ ㄱ . ㅈ ✕ ㅣ ㅗ . ㅋ ㅈ . ㅋ ㅇ ㄱ ㄴ .

ㄱ ✕ ㅗ ㅋ ♡ . ㄱ ㅊ ㅋ ㅇ ㅿㅿ ㅈ ㅿ . ㄱ ㅇ ㅇ . ㄱ 괴 ㄴ . ㅿ ㄱ ㅈ △△ , ㄱ ㅋ ㄱ .

ㅍ 🕮 ㅁ ㅎ ♡ ㅜ . ㅎ ㅊ ㅜ . ✓ ✕ ㅗ ㅎ ♡ . ㅎ ♡ ㅜ = ㅎ ㄱ . ㅋ ㅁ ㅎ ㅅㅈ ㅈ → ㅜ .

🈹 ㄱㅇ ⊙ㅡ ?

ㄴ 🕮 : 🈹 ㅅㅅ ㅅㅅ : ㅅㅅ → ㅅㅅ ㅅㅅ

ㄱㄴ 🕮 : " ㄱㅇ 🙁 。 ㄱㅇ ☹ → 👑 。 👑 ☽ ㄱㅇ 。 " 🈁 ㅅㅅ ㅅㅅ ㅅㅅ : ㅅㅅ

🕴🖖 ㅁ🤘。 ㅎ 🖖 ㅁ🤘。

ㄱ ✕ 🤜 🖧 △ ? 🈹 ㄱ 🤖 ? ㄱ ☺ ? ㄱ ☹ ? ㄱ 😉 🤖 ?

ㄴ 从 ✕ 🗨 ㅁ🤘。 🈹 ㄱㅇ ㅁ🤘? 🈹 ㄱㅇ □ ? 从 ♡ 🕴🖖 。从 ? 🕴🖖 🖃 ㅁ🤘。

ㅅㅅ ? ? 。 🈹 ㅎ ㅁ🤘? 🕴🖖 目 ㄱㅇ。 🕴🖖 ㅁ🤘 土土 。 🕴🖖 ㅁ🤘 ∪∪ 。 🕴🖖 ㅁ🤘 ㅅㅅ 。 🕴🖖 ㅁ🤘 ⊛ 🞩 。 🕴🖖 目 ㅎ ㅁ🤘 ⊛ 土 。

🈹 ㄱㅇ ㅁ🤘? 🕴🖖 🖃 ㅎ ㅁ🤘 △△ ㅎ 🖖 。 🕴🖖 🖃 ㅎ ㅁ🤘 ✕ 。 🕴🖖 🖃 ㅎ ㅁ🤘 ✕ 。

✓目 🈁

ㄴ 🕮 : 🈂 ㅅㅅ ㅅㅅ : ㅅㅅ → ㅅㅅ ㅅㅅ

ㄱㄴ 🕮 : " ㅜ 🤖 目 ㅅㅅ 🐑 。 🤖 ㅅ 。 ㅜ 🤖 目 ㅅㅅ 。 🤖 ㅅ 。 △△ 。 " 🈂 ㅅㅅ ㅅㅅ : ㅅㅅ

ㄱㅇ 目 ㄴ 🖖 ㅇ 。 ㄴ ✕ ✓目 。 ㄴ 🖖 目 。 目 ▯ ㄴ ✓目 🈁 。 ㄱㅇ 🤖 。 🈹 ㅅ ㄴ ✓目 🈁 ? 🕴🖖 ✓目 🈁 ? 🕴🖖 ✓目 🈁 ? 🤖 。 ✕ ✓目 ▫ ? 🕴 ♡ 🖖 ✓目 🈁 。 ▫ 🈁 ✓目 。 🕴 ㅁ ▢ 🈁 ㄱㅇ 。 🕴 🕮 ㅇ 。 🕴 ㅁ ▢ ㅅ ㅈㅈ 🈁 。 ㅎ 🖖 ㅅ △△ 。, ㅁ 🕴 △△ ♡ 🕴🖖 。 ㅜ ✕ ✓目 ▫ , ㅎ ✓目 🈁 。

3 X □

□ 🕮 : 🕮 🫰 从 👣 : 👣 → 👣

ㄱ□ 🕮 : "ㅊ 🖻 ♡ = 🫱 ♡ ㅎ · 🫱 🫴 🫱 🫴 ㅎ · 🫱 ✓ ± 🜲 ᐞᐞ 🔥 → 🤳 · "

🫰 👣 : 🜂

🤳 ☁ □ 😮‍💨 → ㅎ 心心

ㅋ 🫴 从 · 从 ⛲ ㄴ · 🜂 ☾ 从 ⛲ · 从

ㅋ 🫴 ㅅ △△ ᐞᐞ 🫴 ㅿ · 3 X □ · ㅋ 忍 🫴 · 3 ☹ ㅋ ·

✕ 🫴 ? ㅋ ? ☹ · ㅋ □ X ☹ ? 忍 🫴 · ☹ ? 3 X ☹ · ♡ ✳ ㅎ 🫳 · ㅎ 🫳 从 ♡ · ㅎ 🫳 从 目 ♡ ·

🤳 目 ㅎ ♡ ᐞᐞ ♡ · 🤳 ♡ ᐞᐞ ㅎ · ㅎ ♡ ᐞᐞ ㅎ 从 = 🤳 · ㅎ 目 ♡ → 从 ·

🤳 □ ✓

□ 🕮 : 3 🜂 : 🜂 → 🜂 🜂

ㄱ□ 🕮 : "人 △ 🖻 🤳 🕮 · 人 ㅊ 🕸 · 人 🖻 🤳 🕮 ·" 3 🜂 : 🜂 🜂 🤳 ✳ □ ✓

🤳 ✳ □ ✓

ㅋ ♡ ㅋ 🫴 · ㅋ ♡ ㅋ 🫴 □ ✓ · ㅋ □ ㅋ 🫴 ⧖ 🫨 ㅈ · ㅋ ? ㅋ 🫴 ㅈㅈ · ㅋ 🫴 ✳ □ ✓ → ㅋ · 几 从 ✕ □ ✓ → ㅋ · 几 从 ㅍ □ ✓ ✓ △△ · ✕ ㅋ 🫴 · ㅋ 🫴 □ ✓ · ㅋ 🫴 ✓ 🕮🕮 ㅈㅈ ㅋ ·

✓ 从从 □ ✓ · 🙏 ✕ □ 🕮🕮 ㅎ ♡ ↄ · 🙏 □ ✓ → ㅋ · 🕮 □ , ✕ 🖼 从 🫨 🕮🕮 🫥 ㄱ ·

⧖ 🤳 ㅆ 🫴 · △ 🜲 · 🫴 🫴 💧 ㅇ→ 🜲 · 🤳 □ ✓ · 🤳 □ 🫴 ✿ △△ ᐞᐞ 🫳🫳 · 🤳 □ 🫴 ᐞᐞ 🤳 ♡ · 🤳 □ 🫴 ᐞᐞ 🫦 ☹ ·

🤳 ♡ □ → ㅎ · ㅎ 🫳 ⚰ ㅎ 心心 ᐞᐞ ↄ · ㅎ 🕮 🤳 · ㅎ ↄ 🤳 ⧖ ㅎ 🕮 · 🤳 ♡ □ ✓ ᐞᐞ ㅎ 心心 · 🤳 ♡ ㅎ ↄ ✓ ㅇ→ 🤳 · 🤳 ㅈㅈ ㅎ ⧖ ㅎ ? 🤳 · 🤳 🫴 ㅎ ㅈㅈ 🫴 🫨 △△ ·

🤔 🤨

🤔 🤔 : 🕮 🤔 🤦‍♂️ 🤷 🤔 : 🤔 → 🤔

🤔 🤔 : “ 🤷‍♀️ 🤦 🤦 🤔 🤦‍♂️ 🤨 。 🤔 , 🤦 🤦 🤨 🤷 。 🤦 🤷 。 🤦 🤷 🤔 = 🤦 🤷‍♀️ 。 = 🤦 🤷‍♀️ 🤦 。 ” 🤔 🤦‍♂️ 🤷 🤔 : 🤔

🤔 🤷 🤷‍♀️ 🤔 🤔 。 🤔 🤔 🤷 🤷 。 🤷‍♀️ 🤦 。 🤷‍♀️ 🤷 。 🤷‍♀️ 🤷 。 🤷‍♀️ 🤷

🤢 → 🤮

🤔 🕮 : 🕮 📲 🕮 🤷 : 🤷‍♂️ → 🤷‍♂️

🤔 🕮 : “ 🤦 🟥 🤹 , “ 🤞 🤮 🤹 🔼 。“ 🤹 🟥 , “ 🤷 🤮 🤹‍♀️ 🤷‍♂️ 🔽🔽 。🤷 🤮 🤹‍♀️ 🤷 🤷 。🤷 🤮 ➳ 🤴 🔼 🤮 🛞 。“ 📲 🤷 : 🤷‍♂️ 🤷

🤦 🔼 🤞 🤢 🙅 。🤦 🔼 ❌ ✔️ 🖕 。🤞 🙏 🤮 ✔️ 。

🤞 🤮 🤷‍♀️ 🤹‍♀️ 🤹‍♀️ 。🤞 🤮 ❌ ✔️ 🖕 。🤞 🤮 🤹‍♀️ 🤷 🤷‍♀️ 🤹‍♀️ 🤹‍♀️ 。🤞 🤮 🤹‍♀️ 🤷

✕☹♡

◺🕮:⅄🯅⅄:⅄→⅄⅄

⊐◺🕮:"ㅋ♡?🯅⊷♡ㅋ。" ⅄🯅⅄:⅄⅄

ㄇ⊜⊜ㄱ🕯☹⛉。⛉目ㅓㄱ心。?🕯
ㅗ⬭△△。✕从ㄱ•ㅂㅂ。✕回🯅。☹ㅈ,
⊸⊛心。🕯ㄱㅇ→🕯🯅•♡。🕯ㄱ🕯✓
从从。☹🕯ㄱ☹。ᘎ△△☹回。ㄱ△🕮🯅
♡ㄱ。🯅⊃?ㄱ目🯅△△从。ㄱ🝙🯅♡
ㄱ。ㄱ⊰☺。ㄱ⊰♙从•ⓥⓥ⊷。

🯅=♡。(🯅⅄⅄).⋁ㅈ⊿十。⩔目
♡。⋁目⊰♡🕯→⅃).?🯅♡
ㅋ。?🯅ㅈ回ㅋ。ㅋ⊰♡从。
(🯅⅄⅄→⅄⅄)

ㅋ→🕯🯅ㄱ•ㅅ。🯅ㅋ🕯人ㅈ。(⅄⅄→
⅄⅄)。ㅈㅈㅋ🝙🯅•♡。ㅈ🕯ㅋㅍ=🯅。
(🯅⅄⅄→⅄⅄)。ㅋ↑回♡△△⨁。☹⊷
⇉。ㅋ🝙🯅♡ㅋ⩛△△⨷。(🯅⅄→⅄⅄)。

ㅋ🝙🯅♡🕯→ㅋ。ㅋ↑△△🕮。ㅋ↑⊔→
🯅。ㅋ↑⊔→从。ㅋ✕☹。

🯅,ㅇ•♡✕⊸。?ㅇ🝙ㅇ•♡回ㅋ。ㅋ
✕☹♡ㅇ△△从。☺ㅇ。

⊸⩔

◺🕮:⅄🯅⅄:⅄→⅄⅄

⊐◺🕮:"⋁♡人。♡△ㄱ🝙🝙。"
⅄🯅⅄:⅄

ㅋⓥ从。从ⓥㅋ。

ㄱ•🕯⊐⋁☹。☹⊸⅄⊂⅄⅄。ㄱ□
从从,"ㄱⓥㄱ⨯尺🕯⊐。◺从从□ㄱ⊜
⋁ㄱ。🕯⊐☹⅄⊜⊜。ㄱ🕯⨷⨷尺🕯⊐。
✕ㄱ⨯🕯→心→♡。

🯅🯅🕯□ᵔ•从。🯅□,"⋁♡人。"
(⅄🯅⅄:⅄)。ㅅ⩔🯅ᵔ从🯅•△△🕯•
♡。ㅅⓥ♡⋁ㄱ。?🯅🝙🯅•♡回ㅅ•
心心。从♡♡⩔从=。ㅅ目♡尺□🯅,✓
从。❀△△✓□。🯅🕯→🝙。🯅•⊗目从//→
🝙。从🝙⊛从🕯→🯅•?。"🝙⊛△△🕯→🯅•
⩔。🯅•⩔△ᵔ🝙。"(🯅⅄:⅄⅄)⩔🯅•🝙
⓪。🯅⓪🝙•♡△ㅋ。

ㅋⓥ从。从ⓥㅋ。🝙⨯🯅→ㅋ→♡。⊸
⩔。

튼 츄

다 면 : 싫 튄 씲 : 늷 → 싫 씲

ㄱ다 면 : " 튄 회 ㉦ 면 。 면 쇼 ㉥ 회 ✓ 。 ㉥ 회 。 림 ㅎ ⊗ 리 ㅎ 。 ㅈㅈ 。 ㉥ 회 리 쇼 。 " 씲 튄 씲 : 싫 씲

ㅜ 큰 ✓ △△ 리 ㅡ 。 ✕ ✓ 。 ㄲ 쩐쩐 ㅜ ㉥ ㅈ ✓ 。 ㅜ ㉥ 人 。 싫 ⊙ ㅜ 目 탄 。 ㅜ 큰 ✓ △ 냇 。 ㉦ 쇼 。

튄 츄 탄 → ㅅㅅ 튄 。 튄 ↠ 묘 튄 。 튄 目 튄 쇼 。 튄 ▯ ㅇ→ ㉦ 리 ㅍㅍ 。 튄 ▯ , " ㅇ ◒ △△ ㅜ 회 。 ㅇ ◒ △△ ㅜ ㅈ 。 ㅜ ? 。 ㅜ 十 。 ㅜ 쩐 。 ㅜ ♡ 。 ㅜ 쩐 。 ㅜ 艹艹 。 ㅜ 쫀쫀 。 " (싫 튄 씲 : 늷 → 싫 싫) 。 튄 ㉦ 튄 。 ㅇ , 人 리 △△ ㅇ 쩐 회 。 人 리 △△ ㅇ ㉥ 十 。 ㅇ ◒ 从 회 ㅇ 。 ㅇ→ 쩐 ㅇ 큰 。 ㅇ ◒ 人 회 。 (씲 : 싫 씲 → 싫 싫)

튄 ㅈ 目 ㉦ ㉥ ㅎ 。 ㅎ ㉦ 쫀 ㅈ 人 튄 。 튄 □ 튄 회 ㉥ 。 튄 ㉥ 회 。 튄 ㉥ 회 → 회 。 회 目 从 → 从 냇 。

ㅎ ㉦ 튄 ㉥ 쫘 쫘 。 ㅅ ㅈㅈ 十 ㅏ 。 ㅈㅈ ㅎ 从 탄 ㅈ ✓ 。 회 쩐 从 ㅈ ✓ 。 ㅈㅈ 쩐 从 。 쩐 탄 츄 。

从 ㅿ

다 면 : 회 目 싫 : 씲 → 싫 씲

ㄱ다 면 : 目 " ㄱ 目 人 。 ㄱ ⇟ 二 ㅈ 。 人 ㅍ ㄴ ㅿ 人 ㄱ 。 人 □ ✕ 회 。 ㄱ 二 ⊷ 。 ㄱ 二 ⊸ 。 " 目 싫 : 싫 씲

从 ㅿ ↩ ㉦ ㉥ 튄 。 튄 △△ ㅅㅅ 从 탄 。 ✓ 냇 리 쵯 。 쵯 ↣ 냇 。 튄 회 。 튄 ㅅ 리 ㅅ 튄 犬 。 □ ㅈㅈ 면 。 ㅿ ↩ 튄 。 ㅅ 。 ㅅ 。 ㅿ 튄 犬 。 □ ㅈㅈ 면 。 ㅿ ↩ 튄 。 ㅈ 。 ㉦ 回 ✓ 。 튄 ㅅ 튄 。

튄 냇 ㅅ 쇼 。 튄 ↩ 회 ㉥ → ㉦ 。 ? 튄 회 면 。 튄 ㅇ 回 二 쇼 (目 싫 : 늷) 。 튄 目 냇 。 튄 " ⇟ 냇 人 二 ㅈ 。 " 묘 튄 ㉥ ㅎ 쇼 회 。 튄 ▯ , " 냇 ㅍ ㉦ ㅿ ㅜ 。 냇 □ , " ✕ 회 。 ㅜ 二 ⊸ 。 ㅜ 二 ⊸ 。 (싫 씲)

튄 회 ㅎ ✕ ㅎ 。 目 ㅎ ㅇ △△ 。 ㅗ ㅎ 。 튄 ㉥ 쇼 ㅿ ㅎ 。 튄 ✕ ㅣ→ ㅎ 从 。 튄 리 ㅎ 。 튄 ㅿ ㅎ 。 튄 ㅿ ㅎ ㉦ 。 튄 ㉦ 。

🈯🛞✔🈯

🈯🈯:🈯:🈯:🈯:🈯🈯 → 🈯🈯

🈯🈯:"🈯🈯🈯🈯🈯🈯。🈯🈯🈯🈯。🈯🈯🈯🈯。"🈯:🈯🈯

🈯🈯🈯🈯。🈯🈯🈯🈯。🈯🈯🈯🈯。🈯🈯🈯🈯。

3. 5

3.1 Introduction

In this section we will discuss the basic properties of the integers. We will assume that the reader is familiar with the usual arithmetic operations and the ordering relation $<$.

3.2 Definition

A set S is said to be *well-ordered* if every nonempty subset of S has a least element.

3.3 Theorem

The set of positive integers is well-ordered.

3.4 Corollary

Let n be a positive integer. Then there is no integer k such that $n < k < n+1$.

3.5 Theorem

Let a and b be integers with $b \neq 0$. Then there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < |b|$.

3.6 Definition

Let a and b be integers, not both zero. The *greatest common divisor* of a and b, denoted $\gcd(a, b)$, is the largest integer d such that $d \mid a$ and $d \mid b$.

3.7 Lemma

If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

3.8 Proof

Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$, so $d \mid (a - bq)$, that is, $d \mid r$. Hence d is a common divisor of b and r. Conversely, if e is any common divisor of b and r, then $e \mid (bq + r)$, so $e \mid a$. Therefore $e \mid d$, and we conclude that $\gcd(b, r) = d$.

3.9 Example

Find $\gcd(252, 198)$.

$252 = 1 \cdot 198 + 54$

$198 = 3 \cdot 54 + 36$

$54 = 1 \cdot 36 + 18$

$36 = 2 \cdot 18 + 0$

Hence $\gcd(252, 198) = 18$.

3.10 Theorem

Let a and b be integers, not both zero. Then there exist integers x and y such that $\gcd(a, b) = ax + by$.

3.11 Definition

A positive integer $p > 1$ is called *prime* if its only positive divisors are 1 and p. An integer greater than 1 that is not prime is called *composite*.

3.12 Theorem

Every integer $n > 1$ can be written as a product of primes.

3.13 Proof

We use induction on n. If $n = 2$, then n is prime and the result holds. Suppose the result holds for all integers $2 \leq m < n$. If n is prime, we are done. If n is composite, then $n = ab$ with $1 < a < n$ and $1 < b < n$. By the induction hypothesis, a and b are products of primes, so n is also a product of primes.

3.14 Theorem

There are infinitely many primes.

3.15 Proof

Suppose there are only finitely many primes $p_1, p_2, \ldots, p_k$. Let $N = p_1 p_2 \cdots p_k + 1$. Then $N > 1$, so N has a prime divisor p. But p cannot be any of $p_1, \ldots, p_k$, since N leaves remainder 1 when divided by each of them. This contradicts the assumption that $p_1, \ldots, p_k$ were all the primes.

3.16 Definition

The *least common multiple* of a and b, denoted $\operatorname{lcm}(a, b)$, is the smallest positive integer m such that $a \mid m$ and $b \mid m$.

3.17 Theorem

For positive integers a and b, $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

3.18 Example

Find $\operatorname{lcm}(252, 198)$.

Since $\gcd(252, 198) = 18$, we have $\operatorname{lcm}(252, 198) = \frac{252 \cdot 198}{18} = 14 \cdot 198 = 2772$.

3.19 Theorem

Let p be a prime and a an integer. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

3.20 Proof

Consider the set $\{a, 2a, 3a, \ldots, (p-1)a\}$ modulo p. No two of these are congruent, since if $ia \equiv ja \pmod{p}$ with $1 \leq i < j \leq p-1$, then $p \mid (j - i)a$, and since $p \nmid a$ we would have $p \mid (j - i)$, which is impossible. Hence the set is a permutation of $\{1, 2, \ldots, p-1\}$. Multiplying all the elements together gives $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$, and dividing by $(p-1)!$ yields the result.

3.21 Corollary

For any integer a and prime p, $a^p \equiv a \pmod{p}$.

3.22 Definition

Euler's totient function $\varphi(n)$ counts the number of integers $1 \leq k \leq n$ with $\gcd(k, n) = 1$.

3.23 Theorem

If $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$.

3.24 Theorem

Euler's theorem: if $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

3.25 Example

Compute the last two digits of 7^{2024}.

We need $7^{2024} \bmod 100$. Since $\varphi(100) = 40$ and $\gcd(7, 100) = 1$, Euler's theorem gives $7^{40} \equiv 1 \pmod{100}$. Hence $7^{2024} = (7^{40})^{50} \equiv 1^{50} \equiv 1 \pmod{100}$. The last two digits are 01.

3.26 Theorem

The Chinese remainder theorem: if $m_1, m_2, \ldots, m_k$ are pairwise coprime and $a_1, a_2, \ldots, a_k$ are any integers, then the system $x \equiv a_i \pmod{m_i}$ has a unique solution modulo $m_1 m_2 \cdots m_k$.

3.27 Example

Solve $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$.

The solution is $x \equiv 23 \pmod{105}$. Indeed, $23 = 7 \cdot 3 + 2$, $23 = 4 \cdot 5 + 3$, and $23 = 3 \cdot 7 + 2$.

3.28 Definition

A *Mersenne prime* is a prime of the form $2^p - 1$ where p is itself prime.

3.29 Theorem

If $2^p - 1$ is prime, then p is prime.

3.30 Proof

Suppose $p = ab$ with $a, b > 1$. Then $2^p - 1 = (2^a)^b - 1$, which factors as $(2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 1)$. Since $2^a - 1 > 1$, this is a nontrivial factorization of $2^p - 1$, contradicting its primality.

3.31 Theorem

If $2^n + 1$ is prime, then n is a power of 2.

3.32 Proof

Suppose $n = ab$ where b is odd and $b > 1$. Then $2^n + 1 = (2^a)^b + 1$, which factors as $(2^a + 1)(2^{a(b-1)} - 2^{a(b-2)} + \cdots + 1)$. Since $2^a + 1 > 1$, this is a nontrivial factorization of $2^n + 1$, contradicting its primality.

3.33 Definition

A *Fermat prime* is a prime of the form $2^{2^k} + 1$ for some nonnegative integer k.

3.34 Example

The first five Fermat primes are $3, 5, 17, 257, 65537$, corresponding to $k = 0, 1, 2, 3, 4$. It is not known whether any other Fermat primes exist.

3.35 Theorem

Wilson's theorem: an integer $p > 1$ is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.

3.36 Proof

If p is composite, then p has a divisor d with $1 < d < p$, so $d \mid (p-1)!$, and hence $(p-1)! \not\equiv -1 \pmod{p}$. If $p = 2$ or $p = 3$, the congruence holds directly. Suppose $p \geq 5$ is prime. Then the integers $1, 2, \ldots, p-1$ can be paired with their multiplicative inverses modulo p, and the only elements that are their own inverses are 1 and $p-1$. Hence $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$.

3.37 Theorem

If p is an odd prime, then $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

3.38 Definition

The *Legendre symbol* $\left(\frac{a}{p}\right)$ is 1 if a is a quadratic residue modulo p and $p \nmid a$, -1 if a is a quadratic nonresidue modulo p, and 0 if $p \mid a$.

3.39 Theorem

Quadratic reciprocity: if p and q are distinct odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

3.40 Example

Determine whether $x^2 \equiv 5 \pmod{11}$ has a solution.

We compute $\left(\frac{5}{11}\right)$. By quadratic reciprocity, $\left(\frac{5}{11}\right)\left(\frac{11}{5}\right) = (-1)^{2 \cdot 5} = 1$. Since $11 \equiv 1 \pmod{5}$, $\left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$. Hence $\left(\frac{5}{11}\right) = 1$, and the congruence has a solution. Indeed, $4^2 = 16 \equiv 5 \pmod{11}$.

3.41 Theorem

Let p be an odd prime and a an integer with $p \nmid a$. Then $x^2 \equiv a \pmod{p}$ has exactly $1 + \left(\frac{a}{p}\right)$ solutions modulo p.

3.42 Definition

The *Jacobi symbol* $\left(\frac{a}{n}\right)$ for odd $n > 1$ with prime factorization $n = p_1^{e_1} \cdots p_r^{e_r}$ is defined by $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_r}\right)^{e_r}$.

3.43 Theorem

The Jacobi symbol satisfies the reciprocity law $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$ for odd positive integers m and n.

3.44 Example

Compute $\left(\frac{1001}{9907}\right)$.

Using the Jacobi symbol and repeatedly applying reciprocity and reduction, $\left(\frac{1001}{9907}\right) = \left(\frac{9907}{1001}\right) = \left(\frac{901}{1001}\right) = \left(\frac{1001}{901}\right) = \left(\frac{100}{901}\right) = \left(\frac{4}{901}\right) = 1$.

3.45 Theorem

If $\left(\frac{a}{n}\right) = -1$, then $x^2 \equiv a \pmod{n}$ has no solution.

3.46 Proof

Suppose $x^2 \equiv a \pmod{n}$ has a solution. Then $x^2 \equiv a \pmod{p}$ for each prime $p \mid n$, so $\left(\frac{a}{p}\right) = 1$ for each such p. Hence $\left(\frac{a}{n}\right) = \prod_{p \mid n} \left(\frac{a}{p}\right)^{e_p} = 1$, a contradiction.

3.47 Theorem

The converse fails: $\left(\frac{a}{n}\right) = 1$ does not imply that $x^2 \equiv a \pmod{n}$ has a solution.

3.48 Example

$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, but $x^2 \equiv 2 \pmod{15}$ has no solution, since it has no solution modulo 3.

3.49 Theorem

Let n be an odd composite integer and a an integer with $\gcd(a, n) = 1$. If $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$, then n is called an *Euler pseudoprime* to base a.

3.50 Example

$341 = 11 \cdot 31$ is an Euler pseudoprime to base 2, since $2^{170} \equiv 1 \pmod{341}$ and $\left(\frac{2}{341}\right) = \left(\frac{2}{11}\right)\left(\frac{2}{31}\right) = (-1)(-1) = 1$.

3.51 Theorem

If n is an odd composite integer, then n is an Euler pseudoprime to at most $\frac{n-1}{2}$ bases a with $1 \leq a < n$.

3.52 Definition

A *strong pseudoprime* to base a is an odd composite n with $n - 1 = 2^s d$ (d odd) such that either $a^d \equiv 1 \pmod{n}$ or $a^{2^r d} \equiv -1 \pmod{n}$ for some $0 \leq r < s$.

3.53 Theorem

Every strong pseudoprime to base a is an Euler pseudoprime to base a.

3.54 Example

$2047 = 23 \cdot 89$ is a strong pseudoprime to base 2, since $2^{1023} \equiv 1 \pmod{2047}$.

3.55 Theorem

If n is an odd composite integer, then n is a strong pseudoprime to at most $\frac{n-1}{4}$ bases a with $1 \leq a < n$.

3.56 Definition

A *Carmichael number* is a composite n such that $a^{n-1} \equiv 1 \pmod{n}$ for every a with $\gcd(a, n) = 1$.

3.57 Example

$561 = 3 \cdot 11 \cdot 17$ is the smallest Carmichael number.

3.58 Theorem

A composite n is a Carmichael number if and only if n is squarefree and $p - 1 \mid n - 1$ for every prime $p \mid n$.

3.59 Theorem

There are infinitely many Carmichael numbers.

3.60 Theorem

Every Carmichael number is a product of at least three distinct primes.

3.61 Theorem

If n is a Carmichael number, then n is an Euler pseudoprime to every base a with $\gcd(a, n) = 1$.

3.62 Theorem

If n is a Carmichael number, then n is a strong pseudoprime to every base a with $\gcd(a, n) = 1$.

3.63 Theorem

Let n be an odd composite integer. Then n is a Carmichael number if and only if n is squarefree and $\lambda(n) \mid n - 1$, where λ is the Carmichael function.

3.64 Definition

The *Carmichael function* $\lambda(n)$ is the smallest positive integer m such that $a^m \equiv 1 \pmod{n}$ for every a with $\gcd(a, n) = 1$.

3.65 Theorem

If $n = p_1^{e_1} \cdots p_r^{e_r}$, then $\lambda(n) = \operatorname{lcm}(\lambda(p_1^{e_1}), \ldots, \lambda(p_r^{e_r}))$.

3.66 Theorem

For an odd prime power p^e, $\lambda(p^e) = \varphi(p^e) = p^{e-1}(p-1)$.

3.67 Theorem

$\lambda(2) = 1$, $\lambda(4) = 2$, and $\lambda(2^e) = 2^{e-2}$ for $e \geq 3$.

3.68 Example

Compute $\lambda(360)$.

Since $360 = 8 \cdot 9 \cdot 5$, we have $\lambda(360) = \operatorname{lcm}(\lambda(8), \lambda(9), \lambda(5)) = \operatorname{lcm}(2, 6, 4) = 12$.

3.69 Theorem

Carmichael's theorem: $a^{\lambda(n)} \equiv 1 \pmod{n}$ whenever $\gcd(a, n) = 1$.

3.70 Theorem

The Carmichael function satisfies $\lambda(n) \mid \varphi(n)$, with equality if and only if n is 1, 2, 4, an odd prime power, or twice an odd prime power.

3.71 Example

For $n = 15$, $\varphi(15) = 8$ but $\lambda(15) = 4$, so $a^4 \equiv 1 \pmod{15}$ for all a coprime to 15.

3.72 Theorem

If n is a Carmichael number, then $\lambda(n) \mid n - 1$.

3.73 Theorem

Let n be an odd composite integer. If there exists a with $\gcd(a, n) = 1$ and $a^{n-1} \not\equiv 1 \pmod{n}$, then n is not a Carmichael number.

3.74 Example

$n = 91 = 7 \cdot 13$ is not a Carmichael number, since $2^{90} \not\equiv 1 \pmod{91}$.

3.75 Theorem

Let n be an odd composite integer. If n is squarefree and $p + 1 \mid n + 1$ for every prime $p \mid n$, then n is a Carmichael number.

3.76 Example

$n = 561 = 3 \cdot 11 \cdot 17$ is squarefree and $2 \mid 4$, $10 \mid 12$, $16 \mid 16$, so 561 is a Carmichael number.

3.77 Theorem

Let n be an odd composite integer. If n is squarefree and $p + 1 \mid n + 1$ for every prime $p \mid n$, then n is a strong pseudoprime to every base a with $\gcd(a, n) = 1$.

3.78 Theorem

Let n be an odd composite integer. If n is squarefree and $p + 1 \mid n + 1$ for every prime $p \mid n$, then n is an Euler pseudoprime to every base a with $\gcd(a, n) = 1$.

3.79 Theorem

Let n be an odd composite integer. If n is squarefree and $p + 1 \mid n + 1$ for every prime $p \mid n$, then $\lambda(n) \mid n + 1$.

3.80 Theorem

Let n be an odd composite integer. If n is squarefree and $p + 1 \mid n + 1$ for every prime $p \mid n$, then $\lambda(n) \mid \varphi(n)$.

3.81 Theorem

Let n be an odd composite integer. If n is squarefree and $p + 1 \mid n + 1$ for every prime $p \mid n$, then n is a product of at least three distinct primes.

3.82 Theorem

Let n be an odd composite integer. If n is squarefree and $p + 1 \mid n + 1$ for every prime $p \mid n$, then n is a Carmichael number.

3.83 Theorem

Let n be an odd composite integer. If n is squarefree and $p + 1 \mid n + 1$ for every prime $p \mid n$, then n is a strong pseudoprime to every base a with $\gcd(a, n) = 1$.

3.84 Theorem

Let n be an odd composite integer. If n is squarefree and $p + 1 \mid n + 1$ for every prime $p \mid n$, then n is an Euler pseudoprime to every base a with $\gcd(a, n) = 1$.

3.85 Theorem

Let n be an odd composite integer. If n is squarefree and $p + 1 \mid n + 1$ for every prime $p \mid n$, then $\lambda(n) \mid n + 1$.

3.86 Theorem

Let n be an odd composite integer. If n is squarefree and $p + 1 \mid n + 1$ for every prime $p \mid n$, then $\lambda(n) \mid \varphi(n)$.

3.87 Theorem

Let n be an odd composite integer. If n is squarefree and $p + 1 \mid n + 1$ for every prime $p \mid n$, then n is a product of at least three distinct primes.

3.88 Theorem

Let n be an odd composite integer. If n is squarefree and $p + 1 \mid n + 1$ for every prime $p \mid n$, then n is a Carmichael number.

제 1 장

1.1 시작

이 문서는 테스트를 위한 것입니다. 여러 줄의 텍스트가 있습니다.

- 첫 번째 항목
- 두 번째 항목
- 세 번째 항목

1.2 코드

```
def hello():
    print("안녕하세요")
```

1.3 표

이름	나이	직업
김철수	30	개발자
이영희	25	디자이너

1.4 인용

> 인용문입니다.
> 두 번째 줄입니다.

1.5 링크와 이미지

[링크](https://example.com)

1.6 수식

$$E = mc^2$$

1.7 각주

각주[1]

[1] 각주 내용

1.8 마무리

끝.

제 2 장

2.1 시작

이 문서는 테스트를 위한 것입니다. 여러 줄의 텍스트가 있습니다.

- 첫 번째 항목
- 두 번째 항목
- 세 번째 항목

2.2 코드

```
def hello():
    print("안녕하세요")
```

2.3 표

이름	나이	직업
김철수	30	개발자
이영희	25	디자이너

2.4 인용

> 인용문입니다.
> 두 번째 줄입니다.

2.5 링크와 이미지

[링크](https://example.com)

2.6 수식

$$E = mc^2$$

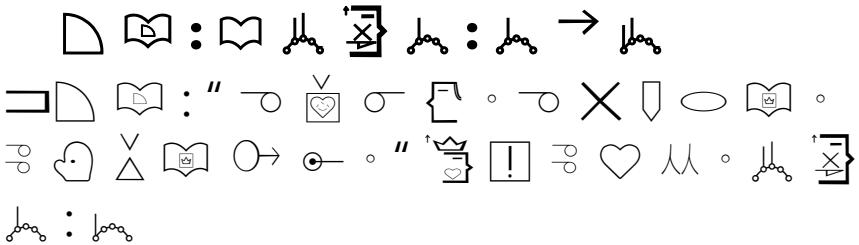
2.7 각주

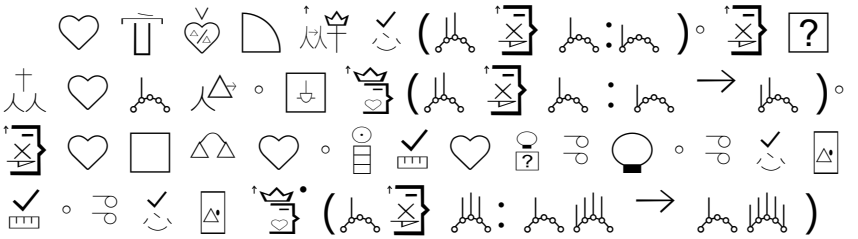
각주[1]

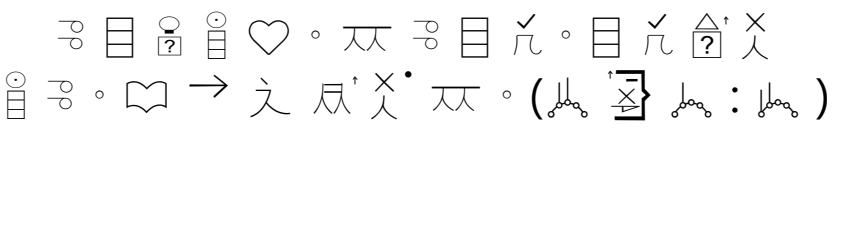
[1] 각주 내용

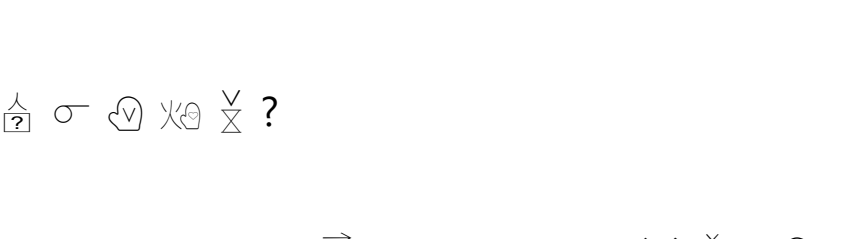
2.8 마무리

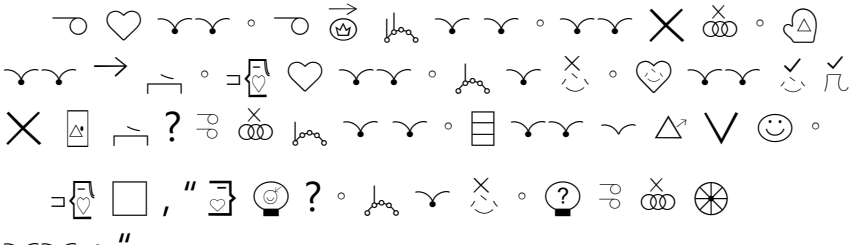
끝.











ㄱㅇ午午ㆍ〉

ㄴ🕮:🕮:ﾑ🏛ㆍ从ﾑ:ﾑﾑ→ﾑﾙ

ㄱㄴ🕮:"🖻✕人🙂→〉人◦🛞⏚✓→

🛞◦"ﾑ🏛ㆍﾑ:ﾑﾑ

从?ㄱ↠ㄱ◦ㅎ🖻ㄱㅇ午午◦ㄱ

☺◦从🤚ㄱ📦◦"✕△?"◦

从□,"✕Ⓥ△◦"ㅎ🛆∞↙↙◦ㅎ

🛆🖻🖻ㅇ午午◦

✕ㄱ目ㅇ午午🖻📦◦午↓↑◦午午

🛆午↓◦

ㅇ午午ㆍ〉ㄱ🙂◦✕✓🙇🙂🙎◦Ⓥ

🙂🛞ㄲ从◦十🖻🗨从Ⓥ✓从从◦

🖻□"🖻,ㅎ🙇ㄱ◦从🤚◦!人🙍◦

从☹Ⓥ🙎◦🙇人◦ㅈㅈ🙆从◦🤚🖾尺

🛞◦"(ﾑ🏛ㆍ从ﾑ:ﾑﾙ)

🖻🙇从ㅁ♡△△〆◦✕人,♡,△△♡

🛆从ㅁ🖻ㆍ△△🛆从🙆◦🙍↑△△🖸🙂

⋁◦从🖞🖻ㆍ🛆从↑◦✕🛆↓◦ㄲ从

⋁↑土◦

🖻ㅈㅈㅎ🙇从◦

✕🜂🙂从〉

ㄴ🕮:🕮🖞ㆍ从ﾑ:ﾑﾑ→ﾑﾙ

ㄱㄴ🕮:"🖻辺→ㄲ◦ㄱ□

🖻⊗◦"🖞ㆍ从ﾑ:ﾑﾑ

从⋁□从◦人□"⏚✕🙂从⧖"◦ㅎ

🖳从〉◦🙂→✕🙂→从⧖⮌◦

ㅁ⧖⧖🖻ㆍ〉🖻🙂◦🖻✓🖞◦🖞🖼

🖻◦(🖻ﾑﾑ:ﾑﾑ→ﾑﾙ)◦🖻✕🗨⋁

(🖻ﾑﾙ:ﾑﾑ→ﾑﾙ)◦🖻从🙇(🖞ㆍ从

ﾑﾑ:ﾑﾑ→ﾑﾙ)◦🖻↔人从◦

🖻↔🙂ㅍㅍ◦(🖞ㆍ从ﾑ:ﾑﾑ→

ﾑﾑ)ㄱ⧖🖻尺☆◦ㄴ🙍🙍□⋁🙍🖞✓

🐑◦🖻✕尺ㅍ✕🐑◦✕↠←→🖻🕮◦

🖻□🖻人◦(🖞ㆍ从ﾑﾙ)

?🖻↣〉,⊸◦🖻⏚🖞🖼✓目人◦

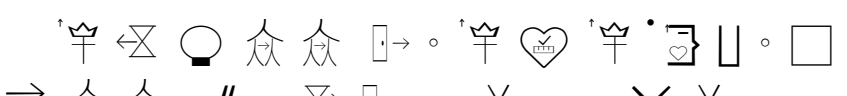
🖞♡🛞从◦

✕人ㅅ🖼〉⧖◦?🖞ㆍ♡,ㅎ🙍♡

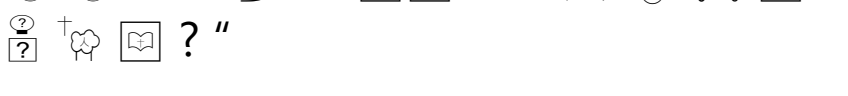
从◦ㅎ🕮🙂从◦ㅎ🖼从⧖Ⓥ◦ㅎ🛞🖞土🖼

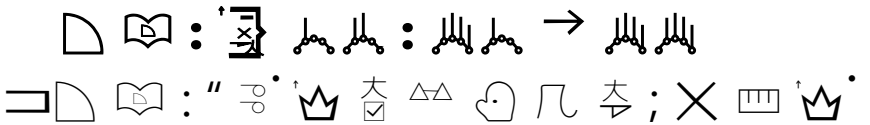
🖞ㆍ♡◦

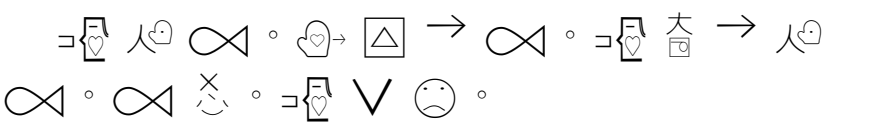
🤔 🤷 🤔

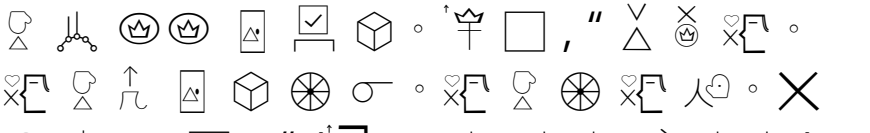


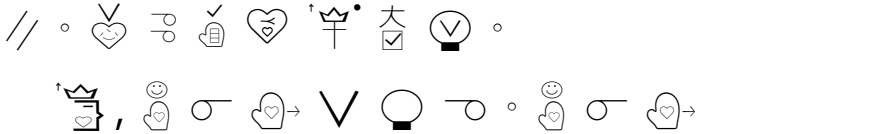
🤔 🤷 🤔 ?

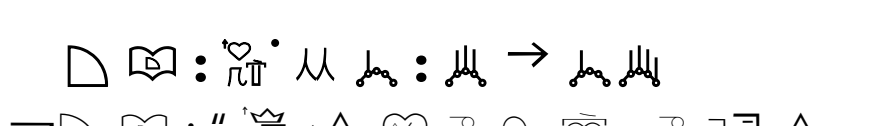


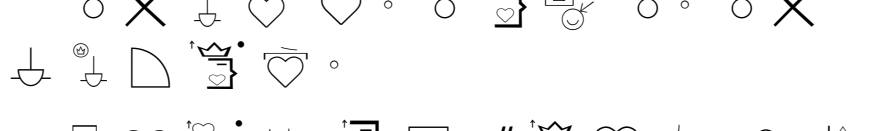












目→土

口🕮:🔣🔣 𝍐𝍐:𝍖→𝍐𝍐

⊐口 🕮:"?ㅎ✕🕹⊛ㅍ丌 ㅛ。ㅎ 𝌆目 ㅍ丌 ×ᛝ 刘。"🔣🔣 𝍐𝍐:𝍐𝍖

▭ 大。ㄱ🔲。ㅎ☹。ㅜㅇ☹。ㅎ目土。ㄱㄱ 𝌆▭□。土🕹☹。🔣人土。🔣🗨 ᛉ☹人🕹。ㅎㄹ目→⊛ᛉ☹。

ㄱ▯🔣🔣 🕮。从ㅇ。从ㅇ🗨☹ 从。ㅏ🖔🕹 从ㅇ→ㄴ。从ㅇ□ᛝ从ᛝ⧖⧖。从ᛝ↑ 尺 ❀ ⧖⧖。从🗨ㄲ 刘。

🔣人ㅍ丌◦从目→🔣•ㅍ丌。ㅍ丌 🔣초。🔣🖔🕹→从。(🔣🔣 𝍐𝍐:𝍖,𝍐𝍖, 𝍐𝍐)🔣从ㅇ?从目🔣•ㅁㅁ。"ㅛㅎ✕🕹⊛ㅍ丌。△▽ㅎ目⊛→刘。"(🔣🔣 𝍐𝍐:𝍐𝍖)

ᛝㅎ•ᛦᛦ ✕ㅅ。ㅎ"㊿㊿◬土。"(🔣🔣 𝍐𝍐:𝍐𝍖)。ㅎ目土🔣•ㅁㅁ。ㅁㅁ ㅈㅈ 乂ㅎ。🔣,⧖ㅎ🕹ᛦᛦ 。ㅈㅈ ㅜ目ㅇ•ㅁㅁ。

✕☹♡

口🕮:𝍐🔣𝍖:𝍖→𝍐𝍐

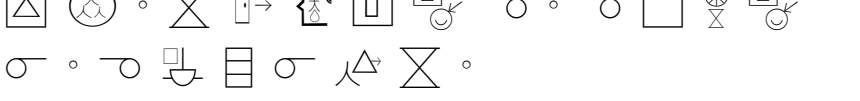
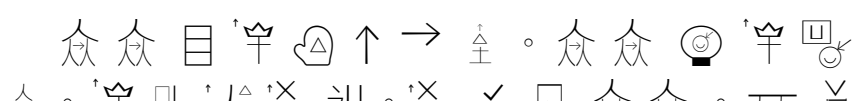
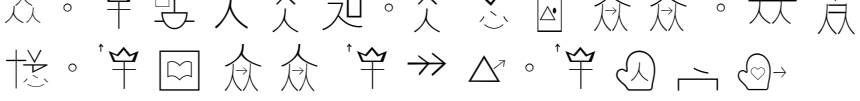
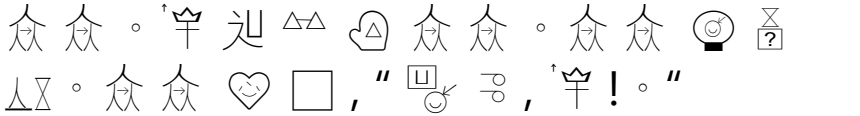
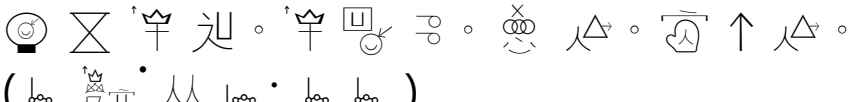
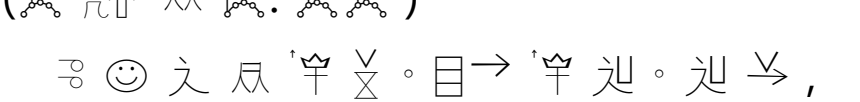
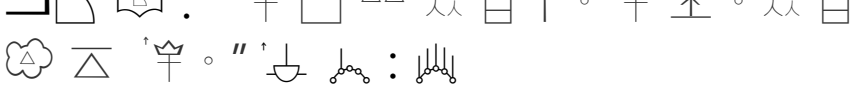
⊐口 🕮:"ㅎ♡?🔣⇢♡ㅎ。"𝍐🔣𝍖:𝍐𝍖

ㅜ🕹☹⛉。⛉目ᛋ ㅜ•心。⛉🕹ㅜ ㄹ⬭ △△。⛉🕹ㅜ从 ㅜ•ㅂㅂ。⛉🕹ㅜ⊡🔣。△▽☹ᛝ,心⇢⊛,△△ᛝ。☹☹🕹ㅜ🗨🔣↑。☹☹🕹ㅜ🗨从。☹人ㅜ☹,☹,ᛝ♡ㄷ。☹人ㅜ☹ 。ㅜ🕮🔣♡ㅜ。🔣⮌?ㅜ□→🔣。⮌ㅜ□→从。?ㅜ🗨🔣♡ㅜ。ㅜ🖔从•ⓥⓥ←△ㅜ•ⓥ。

🔣=♡。(🔣𝍖:𝍐→𝍖)。ᛦ•ᛝ△十。∨大目♡。目ᛉ♡→ㅎ。(🔣𝍖:𝍖→𝍘)。?🔣♡ㅎ。?🔣ᛝ☹ㅎ。ㅎ추♡从。ㅎ🗨?🔣ᛝ。ㅎ🗨🔣←⧖ㅗ。(🔣𝍖:𝍐𝍐→𝍐𝍐)

ㅗㅎ→🕹🔣ㅛ•从ㅛ。🔣ㅛ🕹→ㅎ人🔣ㅅ。(🔣𝍖:𝍐𝍐→𝍐𝍘)。🔣ㅅㅈㅎ🗨🔣•♡。🔣人ㅎ丌目=🔣ㅛ。(🔣𝍖:𝍐𝍐→𝍐𝍖)。ㅎ↑土☹△△㊥。↑土🕹☹。ㅎ✕㊥🔣♡ㅎᛉ。(🔣𝍖:𝍐𝍐→𝍐𝍖)。

ㅎ✓🔣•✿♡🕹→ㅎ。ㅎ↑。ㅎ目从✕☹♡。

🔣,🕹ㅇ🕹→🍵◬◬♡。ᛝㅎ추♡ㅇ。ㅎ추♡从。ㅎ✕☹。

#