

Hemuppgift 1 i 2D1440 Avancerade Algoritmer

Erik Tjernlund
Johan Wilhelmson

16 november 2001

1 Multiplikation

2 Fermats lilla sats

Fermats lilla sats säger att om p är ett primtal, så gäller $a^{p-1} \equiv 1 \pmod{p}$ för heltalet a . För att bevisa detta skriver vi upp de $p - 1$ första multiplerna av a :

$$a, 2a, 3a, \dots, (p-1)a$$

Eftersom vi räknar \pmod{p} är dessa multipler distinkta och skilda från 0. Alltså måste de, i någon ordning, vara kongruenta till:

$$1, 2, 3, \dots, (p-1)$$

Om vi multiplicerar ihop dessa kongruenser får vi:

$$a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p}$$

Omskrivning av detta ger:

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Slutligen dividerar vi med $(p-1)!$ på bägge sidor:

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

3 Primtal

4 Att hitta en cykel i en länkad lista

5 Lemma 4.2

6 Knäcka RSA