Regne ut $a^b \bmod m$

Løse ligninger med mod

$m \mid a$ så er $a^b \bmod m = 0$

$\varphi(m) > b$

Standard metode

Binær metode

$\varphi(m) < b$

mod er primtall

$p \nmid a$

Fermats lille teorem

mod ikke primtall

$a \perp n$

Eulers φ-funksjon $= \varphi(n)$

$a^{\varphi(n)} \equiv 1 \bmod (n)$

Eulers teorem

$m =$ Kvadratfri og $a \not\perp m$

$a^{l \cdot \varphi(n)+1} \equiv a \bmod (m)$

Binær metode

Fermat: $\bmod(p)$ og $p \nmid a$

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

Euler: $\bmod(m)$ og $a \perp m$

$a^{\phi(m)} \equiv 1 \pmod m$

Kvadrat: m kvadratfri og $a \not\perp m$

$a^{l \cdot \phi(m)+1} \equiv a \bmod (m)$

Definisjoner

1 Fermats lille teorem

Formel: Dersom p er et primtal og $p \nmid a$ er

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

2 Eulers φ-funksjon

Formel: Alle naturlige tall som er relativt primske til n og ikke større enn n

3 Eulers teorem

Formel: $$a^{\varphi(n)} \equiv 1 \pmod n$$

Merk: Eulers teorem gjelder bare dersom $a \perp n$

4 Diskrete logaritmer

$$z = \log_y x \iff y^z = x$$

Hvis $b \equiv a^e \bmod m$ så er e den diskrete logaritmen til b med hensyn på basen $a \bmod m$

Oppskrifter

1 Fermats lille teorem

Formel: Dersom p er et primtal og $p \nmid a$ er

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

Eks: $6^{195} \bmod 17$

Ser at $6^{16} \bmod 17 = 1$.

$$6^{195} = 6^{16\cdot 12+3} = (6^{16})^{12} \cdot 6^3 \equiv 1^{12} \cdot 6^3 = 216 \equiv 12 \pmod{17}$$

2 Regne ut $\varphi(n)$

- Primtallsfaktoriser n
- $\phi(p^k) = p^k - p^{k-1}$

Merk: $\varphi(p) = p-1$ for alle primtall p

Eks: $\varphi(17) = 16$

Merk: Funksjonen φ er multiplikativ

$$m \perp n \Rightarrow \varphi(m\cdot n) = \varphi(m) \cdot \varphi(n)$$

Eks:
$$\begin{aligned}\varphi(24) &= \varphi(2^3 \cdot 3) \\ &= \varphi(2^3) \cdot \varphi(3) \\ &= (2^3 - 2^2) \cdot 2 = 4 \cdot 2 \\ &= 8\end{aligned}$$

Eks: $\varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 54$

3

Eulers teorem

- Vi har $a^{\varphi(n)} \equiv 1 \pmod{72}$
- Sjekk at $a \perp n$
- Regn ut $\varphi(n)$
- Gjør om a^n til $a^{\varphi(n) \cdot x}$
- Bruk det at $a^{\varphi(n)} \equiv 1 \pmod{n}$ til å forenkle

Eks: Regne ut $5^{196} \bmod (72)$

Sjekker at $a \perp n$ for å bruke Eulers teorem.

$5 \perp 72$ ✓

Regner ut $\varphi(72)$:

$$\varphi(72) = \varphi(2^3 \cdot 3^2) = (2^3 - 2^2) \cdot (3^2 - 3) = 24$$

Vet derfor at $a^{24} \equiv 1 \bmod (72)$.

$$5^{196} = 5^{24 \cdot 8 + 4}$$

$$5^{196} \bmod (72) = (5^{24})^8 \cdot 5^4 \bmod 72$$

$$\equiv 1 \cdot 5^4 = 49$$

4 Regne ut modulære potensutrykk

- Starter med $a^b \bmod m$
- Regne ut den binære skrivemåten til b
- Regne ut alle $a^d \bmod m$ for d som er i b_2
- $a^b = a^1 \cdot a^2 \cdot a^4 \cdot a^8 \cdot \ldots$
- Skrive om

Eks: Regne ut $36^{83} \bmod 125$

83 i binær $= 1010011$ $(64 + 16 + 2 + 1)$

Regner ut alle potenser i 2 tallssystemet for 36

$36^1 = 36 \equiv 36$

$36^2 = 36^2 = 1296 \equiv 46$

$36^4 = 46^2 = 2116 \equiv 116$

$36^8 = 116^2 = 13456 \equiv 81$

$36^{16} = 81^2 = 6561 \equiv 61$

$36^{32} = 61^2 = 3721 \equiv 96$

$36^{64} = 96^2 = 91$

$$36^{83} = 36^{64} \cdot 36^{16} \cdot 36^2 \cdot 36^1 \equiv 91 \cdot 61 \cdot 46 \cdot 36 \equiv 81$$