7.3 Eulers teorem

Fra sist: (1) Eulers phi-funksjon:

$$\phi(n) = \text{antall } a \in \{1,2,\dots,n\} \text{ med } \gcd(a,n)=1$$

(2) Hvis $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$:

$$\phi(n) = n(1-1/p_1)(1-1/p_2)\cdots(1-1/p_t)$$

Fermats teorem: Hvis p er prim og p ta sier FT at $a^{p-1} \equiv 1 \pmod p$. Antagelse pta er ekvivalent med $\gcd(a,p)=1$ siden p er prim, og $p-1 = \phi(p)$. Så FT kan reformuleres slik: hvis p er prim og $\gcd(p,a)=1$, så gjelder

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

Eulers teorem generaliserer dette.

Lemma: La $n \geq 1$ og $\gcd(a,n)=1$. La $b_1, b_2, \dots, b_{\phi(n)}$ være de $\phi(n)$ tallene i mengden $\{1,2,\dots,n\}$ som er rel. pr. med n. Da er tallene

$$ab_1, ab_2, \dots, ab_{\phi(n)}$$

kongruente med tallene $b_1, b_2, \dots, b_{\phi(n)}$ modulo n, i en eller annen rekkefølge.

Bevis: Se på ab_i for en $1 \leq i \leq \phi(n)$. La $1 \leq b \leq n$ være det unike tallet med $ab_i \equiv b \pmod n$. Siden $\gcd(a,n)=1$ og $\gcd(b_i,n)=1$, er også $\gcd(ab_i,n)=1$ (hvorfor?). Men da er også $\gcd(b,n)=1$ (hvorfor?). Så $b \in \{1,2,\dots,n\}$ og er rel. pr. med n, altså er $b \in \{b_1, b_2, \dots, b_{\phi(n)}\}$. Følgelig er ab_i kongr med ett av tallene $\{b_1, b_2, \dots, b_{\phi(n)}\}$.

Kan to ulike av tallene $ab_1, ab_2, \dots, ab_{\phi(n)}$ være kongr med det samme tallet i $\{b_1, b_2, \dots, b_{\phi(n)}\}$? Hvis ja, vil det finnes $i \neq j$ med

$$ab_i \equiv ab_j \pmod n$$

Men $\gcd(a,n)=1$, så vi kan dele ut a og få

$$b_i \equiv b_j \pmod n$$

Dette er umulig siden b_i og b_j ligger i mengden $\{1,2,\dots,n\}$. □

Eksempel: Se på $n=10$. Her $\phi(10)=4$, og tallene $1,3,7,9$ er de fire tallene i mengden $\{1,2,\dots,10\}$ som er rel. pr. med 10. Siden $\gcd(3,10)=1$, sier lemmaet at tallene $3\cdot1, 3\cdot3, 3\cdot7, 3\cdot9$ er kongr med $1,3,7,9$ modulo 10, i en eller annen rekkefølge. Sjekk dette.

Teorem 7.5 (Eulers teorem)

Hvis $n \geq 1$ og $\gcd(a,n)=1$, så er

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

Bevis: La $b_1, b_2, \ldots, b_{\phi(n)}$ være de $\phi(n)$ tallene i mengden $\{1,2,\ldots,n\}$ som er rel. pr. med n. Fra lemmaet er da de $\phi(n)$ tallene $ab_1, ab_2, \ldots, ab_{\phi(n)}$ kongruente med $b_1, b_2, \ldots, b_{\phi(n)}$ i en eller annen rekkefølge. Da får vi $\phi(n)$ kongruenser av typen

$$ab_i \equiv b_j \pmod{n}$$

og når vi multipliserer dem sammen får vi

$$(ab_1)(ab_2)\cdots(ab_{\phi(n)}) \equiv b_1 b_2 \cdots b_{\phi(n)} \pmod{n}$$

Hvis vi setter $b = b_1 b_2 \cdots b_{\phi(n)}$ har vi altså

$$b \cdot a^{\phi(n)} \equiv b \pmod{n}.$$

Men $\gcd(b,n)=1$ (hvorfor?), så vi kan dele ut b og få

$$a^{\phi(n)} \equiv 1 \pmod{n}$$ □

Merk: (1) Fermats teorem er et spesialtilfelle.

(2) ET kan også vises vha binomialteoremet (se alternativt bevis i læreboken).

Eksempler: (1) Siden $\gcd(-5,72)=1$ gir ET at $(-5)^{\phi(72)} \equiv 1 \pmod{72}$. Har $72 = 2^3 \cdot 3^2$, så $\phi(72) = 2^3 \cdot 3^2 (1-\frac{1}{2})(1-\frac{1}{3}) = 24$. Altså:

$$(-5)^{24} \equiv 1 \pmod{72}$$

(2) Eksamen V2004, oppg 3.

(a) La $a \in \mathbb{Z}$ og $n \in \mathbb{N}$ med $\gcd(a,n)=1$. Vis vha ET at det finnes en $b \in \mathbb{Z}$ med $ab \equiv 1 \pmod{n}$. Finn en slik b for 16 modulo 35.

(b) Hva får vi til rest når vi deler 80^{241} på 77?

For (a), siden $\gcd(a,n)=1$ gir ET at $a^{\phi(n)} \equiv 1 \pmod{n}$, dvs

$$a \cdot a^{\phi(n)-1} \equiv 1 \pmod{n}$$

Så $b = a^{\phi(n)-1}$ har egenskapen $ab \equiv 1 \pmod{n}$. Merk at $\phi(n)-1 \geq 0$, så $b \in \mathbb{Z}$. Siden $\gcd(16,35)=1$ er $16^{\phi(35)} \equiv 1 \pmod{35}$. Har $35 = 7 \cdot 5$ så $\phi(35) = (7-1)(5-1) = 24$, så $16 \cdot 16^{23} \equiv 1 \pmod{35}$. Altså er $b = 16^{23}$ en slik b for 16 modulo 35.

For (b), siden $\gcd(80,77)=1$ gir ET at $80^{\phi(77)} \equiv 1 \pmod{77}$.
Har $\phi(77) = \phi(7\cdot 11) = (7-1)(11-1) = 60$, så

$$80^{60} \equiv 1 \pmod{77}.$$

Det gir

$$80^{240} \equiv (80^{60})^4 \equiv 1^4 \equiv 1 \pmod{77}$$

og videre

$$80^{241} \equiv 80 \cdot 80^{240} \equiv 80 \cdot 1 \equiv 3 \pmod{77},$$

så resten blir 3.