Fermats lille teorem og Eulers phi-funksjon

Introduksjon

I denne oppgaven introduserer vi to teoremer og noen regneoppgaver som er nesten uløselige uten disse teoremene. Men før vi kan introdusere dem, trenger vi litt notasjon. Slik skriver vi f.eks. at et resultat gjelder "modulo 6": $8 \equiv 2 \pmod 6$ eller $-13 \equiv 1 \pmod 7$. Da kan vi skrive ned teoremene våre.

Fermats lille teorem

Det første heter Fermats lille teorem, og er mye brukt i tallteori og i tallteori-oppgaver på mattekonkurranser. Det finnes to ekvivalente måter å si det på. Her er a et heltall og p et primtall:

$$a^p \equiv a \pmod p, \text{eller}$$
$$a^{p-1} \equiv 1 \pmod p$$

Dette teoremet sier altså at et tall opphøyd i et primtall er ekvivalent med tallet modulo primtallet. Nå lurer du kanskje på hva dette skal være godt for, og det er kanskje ikke så lett å se, så derfor løser vi en eksempeloppgave som er typisk for mattekonkurranser:

Spørsmål: Hva er $169 \pmod 3$?

Svar: $169 = 13^2$, så $169 = 13^{3-1} \equiv 1 \pmod 3$

En annen nyttig ting som Fermats lille kan brukes til er *kryptering*. I RSA-algoritmen, som man bruker for å gjøre f.eks. nettbank trygt, brukes Fermats lille teorem til å utveksle informasjon.

Eulers teorem

Eulers teorem er en generalisering av Fermats teorem, og gjør bruk av Eulers phi-funksjon, som er definert slik: $\phi(n)$ er alle tall $< n$ som er *relativt primiske* til n, dvs. alle tall som ikke deler noen felles faktorer med n. Det er da enkelt å se at $\phi(p) = 1$ for alle primtall p. Vi kan da skrive ned Eulers teorem, som gjelder for alle positive heltall a og n som ikke har noen felles faktorer (er relativt primiske):

$$a^{\phi n} \equiv 1 \pmod n$$

Dette er enda mer anvendelig enn Fermats lille. Vi kan f.eks. løse dette:

Spørsmål: Hva er det siste sifferet i 7^{2009}?

Svar: 7 og 10 er relativt primiske, så vi kan bruke Eulers teorem. $\phi(10) = 4$, og $7^{2009} = 7^{4 \cdot 502+1} = (7^4)^{502} \cdot 7^1 \equiv 1^{502} \cdot 7 \pmod{10}$. Altså vet vi at det siste tallet i 7^{2009} er 7. Prøv å løse det problemet uten å kunne Eulers teorem, og du får litt hodebry.

Problemet

Her kommer det tre små oppgaver til å begynne med, for å sjekke at du har kontroll på hvordan disse teoremene virker. Så kommer et ganske enkelt bevis for å sjekke at du kan bruke teoremene abstrakt, og til slutt kommer et vanskelig bevis.

1: Regn ut $289 \pmod 3$.

2: Finn ut om 531441 er delelig med 3.

3: Finn resten når 52^326 deles på 42.

4: Bevis at Fermats lille teorem er et spesialtilfelle av Eulers teorem.

5: Vis at $(p-1)! \equiv -1 \pmod p$ hvis p er et primtall.

Tips

Se på polynomet $g(x) = (x-1)(x-2)...(x-(p-1))$ og polynomet $f(x) = g(x) - (x^{p-1} - 1)$. Du kan bruke at et n-te grads polynom har n røtter også når vi regner modulo i dette spesielle tilfellet. Se på polynomet $f(x)$. Hvor mange røtter har det? Kan du bruke Fermats lille teorem til å finne antall røtter av $f(x)$? Du kan bruke at $\phi(mn) = \phi(m)\phi(n)$ En selvmotsigelse om antall røtter vil kanskje si at $f(x) \equiv 0 \pmod p$? Se nå på konstantleddet i $f(x)$, dvs. når $x = 0$, og vi fortsatt vet hva $f(x) \pmod p$ er.

Dette teoremet heter Wilson's teorem og er et vakkert resultat i tallteori.