Onsdag 11/4-12

Sætning 4.5.4 For ulhardvist $n \in \mathbb{Z}$, $n \geq 2$. findes der uendelig mange primtal p så $p \equiv 1 \pmod{n}$

Bevis

Del 1 Antag, at der for hvert $n \geq 2$ findes mindst et primtal som kongruent til 1 modulo n.

Antag, at der findes endelig mange sådanne. Lad p være det største.

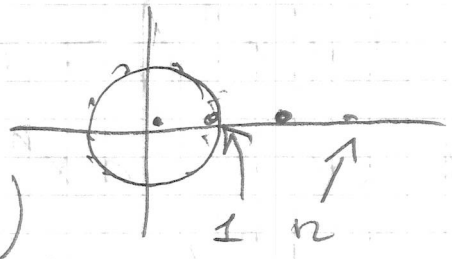
Der findes primtal q som kongruent til 1 modulo $p \cdot n$. Men $q > p \cdot n > n$ og selvfølgelig q kongruent til 1 modulo n. Modsigelse.

Del 2 (eksistens af et p)

Lad n være givet.

$$|\Phi(n)| > 1$$

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - e^{k \frac{2\pi}{n} i})$$



For $n = 2$ $\Phi_2(x) = x + 1$ så $\Phi_2(2) = 3$

For $n > 2$ er hvert led ovenfor af norm mere end 1.

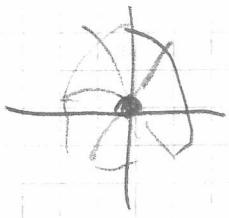
9/10 3/7

Da $\Phi_n(x)$ har heltalskoefficienter haves

$$|\Phi_n(n)| \in \mathbb{Z}, \quad |\Phi_n(n)| \geq 2 \quad \text{og}$$

dermed findes primtal p så

$$p \mid \Phi_n(n).$$



$$|\Phi_n(0)| = 1$$ den norm af

$$\left(0 - e^{k\frac{2\pi}{n}i}\right) \text{ lig } 1$$

så Φ_n har konstantled lig ± 1

altså $\Phi_n(n) \equiv \pm 1 \pmod{n}$

Dermed $p \nmid n$., og derfor

$$D(x^n - 1) = n x^{n-1} \neq 0$$

Eneste rod i $n x^{n-1}$ er 0 som ej rod i $x^n - 1$ så $x^n - 1$ har ingen multiple rødder i $\mathbb{F}_p$

Opsummering: ∘ $\Phi_n([n]) = 0$ i $\mathbb{F}_p$

4/7 10/10

∘ $[n]$ ej multipel rod i $x^n - 1$

men så $[n]$ primitiv n'te enheds rod. i $\mathbb{F}_p$

Et elements orden går op i gruppens orden (gruppen er $\mathbb{F}_p^*$)