Ett bevis för kvadratiska reciprocitetsatsen

Inga bevis för kvadratiska reciprocitetssatsen är särskilt korta, även om en del är elementära. I min jakt på bra bevis har jag fastnat för ett som belyser grundläggande principer i den elementära talteorin, t ex den monumentalt användbara Kinesiska Restsatsen. Vidare kommer Wilsons sats och Eulers Kriterium in på ett naturligt och belysande sätt.

Beviset är av Rousseau, och jag har redigerat det från en övningsuppgift i en lärobok.

Beviset utgår från två "halva" restsystem modulo pq där p, q är två givna, olika, udda primtal. "Halv" betyder att varje heltal, som ej är delbart med p eller q, är kongruent med antingen plus eller minus något t i systemet, och att exakt det ena fallet gäller. Vi behåller därvid alltså endast de invertibla klasserna. Antalet sådana är $\phi(pq) = (p-1)(q-1)$. Antalet element i våra halva restsystem är alltså $(p-1)(q-1)/2$

Ett sådant halvsystem utgöres av de $t = 1, 2, \ldots, (pq-1)/2$ som inte är delbara med vare sig p eller q. Obs att

$$pq - k \equiv -k \pmod{pq}$$

för alla k. Om $k > (pq-1)/2$ så är $pq - k \leq (pq-1)/2$.

Ett annat får vi om vi sätter $u_p = 1, 2, \ldots p-1$ och $u_q = 1, 2, \ldots (q-1)/2$ och löser kongruenssystemen

$$u \equiv u_p \pmod{p}$$

$$u \equiv u_q \pmod{q}$$

som ju är entydigt lösbara modulo pq. Obs. att för dessa u gäller att:

$$-u \equiv p - u_p \pmod{p}$$

$$-u \equiv -u_q \equiv q - u_q \pmod{q}$$

där det första högerledet är av ovan angivet slag, medan det andra liger i komplementet till de angivna resterna modulo q. Således utgör även dessa u ett "halvt" restsystem.

Om $t \equiv \pm u \pmod{pq}$ (t och u hör här till respektive halvsystem) så gäller förstås $t \equiv t_p \equiv \pm u_p \pmod{p}$ och $t \equiv t_q \equiv \pm u_q \pmod{q}$ med *samma* tecken i båda fallen. Produkten av alla t är då kongruent med ett visst tecken gånger produkten av alla u modulo både p och q, med samma tecken i båda fallen. Bestämningarna av tecken och produkter kommer då att ge oss reciprocitetssatsen.

EXEMPEL. Innan vi går vidare till beviset exemplifierar vi med $p = 3, q = 5$. Här är $t = 1, 2, 4, 7$ med produkten $56 \equiv -1 \pmod{3}$ och $\equiv 1 \pmod{5}$. Vi har $u_p = 1, 2; u_q = 1, 2$. Lösning av kinessystemet ger oss (egentligen behöver vi inte bestämma u)

$$\begin{pmatrix} u_p & u_q & u \\ 1 & 1 & 1 \\ 1 & 2 & 7 \\ 2 & 1 & 11 \\ 2 & 2 & 2 \end{pmatrix}$$

Obs. att $11 \equiv -4 \pmod{pq}$ medan de övriga elementen är desamma. Mycket riktigt blir produkten av alla u_p kongruent med $4 \equiv 1 \pmod 3$ och produkten av alla u_q kongruent med $4 \equiv -1 \pmod 5$, alltså ombytta tecken i båda fallen.

Vi lämnar exemplet och övergår nu till vårt **BEVIS**.

Produkten av alla u_p

Först beräknar vi produkten av alla u_p. Alla rester $u_p = 1, 2, \ldots p-1$ förekommer i det första högerledet lika många gånger som det finns högerled u_q i den andra kongruensen, dvs. $(q-1)/2$ gånger. Således är

$$\Pi u_p \equiv (p-1)!^{(q-1)/2} \equiv (-1)^{(q-1)/2} \pmod p$$

där vi använt Wilsons sats.

Produkten av alla u_q

Sedan beräknar vi produkten av alla u_q. Vi behöver då iakttagelsen

$$(q-1)! \equiv (-1)^{(q-1)/2}((\frac{q-1}{2})!)^2$$

som vi erhåller genom att para ihop faktorerna i $(q-1)!$ utifrån och in, en ide som kommer in i många av lärobokens bevis: $q-k \equiv -k \pmod q$. Jämför beviset för Gauß' Lemma.

Vartochett av de $(q-1)/2$ högerleden u_q förekommer lika många gånger som det finns vänsterled u_p, dvs. $p-1$ gånger. Således gäller:

$$\Pi u_q \equiv ((q-1)/2)!)^{p-1} \equiv ((-1)^{(q-1)/2}(q-1)!)^{(p-1)/2} \equiv (-1)^{(q-1)(p-1)/4} \cdot (-1)^{(p-1)/2} \pmod q$$

Det sista steget kommer ur en ny tillämpning av Wilson.

Produkten av alla t_p och alla t_q

Vi går nu till produkterna av alla t_p och t_q. Här råder full symmetri så vi behöver bara beräkna den ena i noggrann detalj.

Det underlättar att fylla ut Πt_p med faktorerna $q, 2q, \ldots q(p-1)/2$ alltså de faktorer, delbara med q, vilka vi utelämnat.

Vi beräknar alltså produkten

$$q \cdot 2q \cdots \frac{p-1}{2} q \, \Pi t_p \equiv q^{(p-1)/2}(\frac{p-1}{2})! \Pi t_p \equiv (\frac{q}{p})(\frac{p-1}{2})! \, \Pi t_p \pmod p$$

Denna får vi genom att multiplicera alla tal från 1 till $(pq-1)/2$, utom att vi hoppar över $p, 2p$, osv. Nu är antalet faktorer lika med de ursprungliga plus $(p-1)/2$ extra, lika med

$$\frac{(p-1)(q-1)}{2} + \frac{p-1}{2}$$

Faktorerna kommer därför att sorteras i $(q-1)/2$ grupper, med $p-1$ faktorer, vilka alla är kongruenta med $(p-1)!$ (modulo p), samt en sista grupp med $(p-1)/2$ faktorer, kongruent med $(\frac{p-1}{2})!$. Obs, t ex, att

$$(mp+1)(mp+2)\ldots((m+1)p-1) \equiv (p-1)! \pmod p$$

Faktorn $((p-1)/2)!$ kan vi kancellera ur båda leden, så vi erhåller

$$\left(\frac{q}{p}\right)\Pi t_p \equiv ((p-1)!)^{(q-1)/2} \equiv (-1)^{(q-1)/2} \pmod{p}$$

efter ännu en tillämpning av Wilson.

Genom att låta p och q byta roller får vi på samma sätt:

$$\left(\frac{p}{q}\right)\Pi t_q \equiv ((q-1)!)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{q}$$

Vi ser nu att $\Pi t_p \equiv \pm\,\Pi u_p \pmod{p}$ där tecknet $\pm$ i högerledet ges av legendresymbolen (q/p).

Således gäller $\Pi t_q \equiv \pm\Pi u_q \pmod{q}$ med samma tecken. Vi kombinerar detta med de funna uttrycken ovan:

$$\left(\frac{p}{q}\right)\Pi t_q \equiv ((q-1)!)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{q},$$

$$\Pi t_q \equiv \left(\frac{p}{q}\right)(-1)^{(p-1)/2} \pmod{q},$$

$$\Pi u_q \equiv (-1)^{(q-1)(p-1)/4} \cdot (-1)^{(p-1)/2} \pmod{q}$$

Det ena uttrycket är alltså (q/p) gånger det andra. Efter kancellation av faktorn $(-1)^{(p-1)/2}$ erhåller vi så äntligen den önskade satsen. Obs. att båda leden är plus eller minus ett, så kongruens modulo q kan bytas mot likhet:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$$