Notes on quadratic reciprocity

1. Let $p \geq 3$ be an odd prime number. Let $S_p := \{1,2,3,\ldots,(p-1)2\}$. For every integer a such that $\gcd(a,p) = 1$, define

$$T(a,p) := \{i \in S_p \mid r_i := ai - \lfloor ai/p \rfloor \geq (p+1)/2\},$$

$$T'(a,p) := \{i \in S_p \mid r_i := ai - \lfloor ai/p \rfloor \leq (pq1)/2\}.$$

Let $\mu(a,p) := \#T(a,p)$. It is easily verified that

$$S(p) = \{r_i \mid i \in T'(a,p)\} \cup \{p - r_i \mid i \in T(a,p)\},$$

a key observation. Hence

$$a^{(p-1)/2} \cdot \prod_{1 \leq i \leq (p-1)/2} i = \prod_{1 \leq i \leq (p-1)/2} (ai) \equiv (-1)^{\mu(a,p)} \cdot \prod_{1 \leq i \leq (p-1)/2} i \pmod{p}.$$

Therefore $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv (-1)^{\mu(a,p)} \pmod{p}$, and we conclude that

$$\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)} \tag{1}$$

for every integer a which is prime to p. The last displayed equality is called "Gauss's criterion" (Theorem 23.1 in the 4th edition). In the case $a = 2$, formula (1) gives

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/2} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases} \tag{2}$$

2. For each $i \in S(p)$, if remainder $r_i \leq (p-1)/2$ then $\lfloor 2r_i \rfloor = 0$, while $\lfloor 2r_i \rfloor = 1$ if $r_i \geq (p+1)/2$. Since $2ai = 2\lfloor \frac{ai}{p} \rfloor p + 2r_i$, we have $\left\lfloor \frac{2ai}{p} \right\rfloor = 2\left\lfloor \frac{ai}{p} \right\rfloor + \left\lfloor \frac{2r_i}{p} \right\rfloor$, we have

$$i \in T(a,p) \text{ if and only if } \left\lfloor \frac{2ai}{p} \right\rfloor \equiv 1 \pmod{2},$$

which implies that

$$\mu(a,p) \equiv \sum_{1 \leq i \leq (p-1)/2} \left\lfloor \frac{2ai}{p} \right\rfloor \pmod{2}.$$

Therefore Gauss's criterion can be restated as

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{1 \leq i \leq (p-1)/2} \left\lfloor \frac{2ai}{p} \right\rfloor} \tag{3}$$

3. We can get rid of the "2" in the exponent "$\left\lfloor \frac{2ai}{p} \right\rfloor$" appearing in formula (3) above. The discussion depends on the parity of the integer a.

Suppose first that $a = 2b$ is even. We get from the multiplicativity of the Legendre symbol that

$$\left(\frac{a}{p}\right) = \left(\frac{2b}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{2}{p}\right) \cdot (-1)^{\sum_{1 \leq i \leq (p-1)/2} \left\lfloor \frac{2ai}{p} \right\rfloor} = \left(\frac{2}{p}\right) \cdot (-1)^{\sum_{1 \leq i \leq (p-1)/2} \left\lfloor \frac{ai}{p} \right\rfloor} \tag{4}$$

for every even integer a prime to p.

Suppose next that a is odd. Then $a+p$ is even, and $\left(\frac{a}{p}\right)=\left(\frac{a+p}{p}\right)$. So we can apply formula (4)

$$\left(\frac{a}{p}\right)=\left(\frac{a+p}{p}\right)=\left(\frac{2}{p}\right)\cdot(-1)^{\sum_{1\le i\le(p-1)/2}\left\lfloor\frac{(a+p)i}{p}\right\rfloor}.$$

In the above formula, we have $\left\lfloor\frac{(a+p)i}{p}\right\rfloor=\left\lfloor\frac{ai}{p}+i\right\rfloor$ for every i, therefore

$$\sum_{1\le i\le(p-1)/2}\left\lfloor\frac{(a+p)i}{p}\right\rfloor=\sum_{1\le i\le(p-1)/2}\left\lfloor\frac{ai}{p}\right\rfloor+\sum_{1\le i\le(p-1)/2}=\sum_{1\le i\le(p-1)/2}\left\lfloor\frac{ai}{p}\right\rfloor+\frac{p^2-1}{8}.$$

We conclude that

$$\left(\frac{a}{p}\right)=(-1)^{\sum_{1\le i\le(p-1)/2}\left\lfloor\frac{ai}{p}\right\rfloor}\cdot(-1)^{(p^2-1)/8}\cdot\left(\frac{2}{p}\right) \tag{5}$$

for every odd integer a prime to p.

Setting a to 1 in (5), we recover the formula (2) for the Legendre symbol $\left(\frac{2}{p}\right)$. We simplify formulas (4) and (5) using (2) as

$$\left(\frac{a}{p}\right)=\begin{cases}(-1)^{\sum_{1\le i\le(p-1)/2}\left\lfloor\frac{ai}{p}\right\rfloor} & \text{if } a \text{ is odd}\\ (-1)^{\sum_{1\le i\le(p-1)/2}\left\lfloor\frac{ai}{p}\right\rfloor}\cdot(-1)^{\frac{(p^2-1)}{8}} & \text{if } a \text{ is even}\end{cases} \tag{6}$$

for every integer a with $\gcd(a,p)=1$. Note that the sum $\sum_{1\le i\le(p-1)/2}\left\lfloor\frac{ai}{p}\right\rfloor$ is equal to the number of all pairs (i,j) of integer i,j with $1\le i<p/2$ and $j\le ai/p$, or equivalently $pj\le ai$:

$$\sum_{1\le i\le(p-1)/2}\left\lfloor\frac{ai}{p}\right\rfloor=\#\{\,(i,j)\mid 1\le i\le p/2,\ 1\le j\le a/2,\ pj<ai\} \tag{7}$$

4. Suppose that q is an odd prime number, $q\ne p$. From (7) we have

$$\sum_{1\le i\le(p-1)/2}\left\lfloor\frac{qi}{p}\right\rfloor=\#\{\,(i,j)\mid 1\le i\le p/2,\ 1\le j\le q/2,\ pj<qi\} \tag{8}$$

and

$$\sum_{1\le j\le(q-1)/2}\left\lfloor\frac{pj}{q}\right\rfloor=\#\{\,(j,i)\mid 1\le j\le q/2,\ 1\le i\le p/2,\ qi<pj\} \tag{9}$$

Clearly

$$\#\{\,(j,i)\mid 1\le j\le q/2,\ 1\le i\le p/2,\ qi<pj\}=\#\{\,(i,j)\mid 1\le j\le q/2,\ 1\le i\le p/2,\ qi<pj\}, \tag{10}$$

Consider set U consisting of all pair (i,j) of integers with $0<i<p/2$ and $0<j<q/2$. Clearly every element $(i,j)\in U$ satisfies either $pj<qi$ or $qi<pj$: if $pj=qi$, then $p|i$ and $q|j$, which is absurd because $0<i<p/2$ and $0<j<q/2$. Therefore

$$\sum_{1\le i\le(p-1)/2}\left\lfloor\frac{qi}{p}\right\rfloor+\sum_{1\le j\le(q-1)/2}\left\lfloor\frac{pj}{q}\right\rfloor=\#U=\tfrac{p-1}{2}\cdot\tfrac{q-1}{2} \tag{11}$$

From (6) and (11) we conclude that

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \tag{12}$$

for any two odd prime numbers $p\ne q$. We have proved the *quadratic reciprocity law*.