b) $\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right)\left(\frac{73}{383}\right) = -\left(\frac{383}{3}\right)\left(\frac{383}{73}\right) = -\left(\frac{2}{3}\right)\left(\frac{18}{73}\right) = -\left(\frac{18}{73}\right) =$

383 Primzahl

$\left(\frac{2}{73}\right)\left(\frac{9}{73}\right) = \left(\frac{2}{73}\right) = 1$ (2. Erg.satz)

also $X^2 \equiv 219$ mod 383 lösbar.

Bem. Um $\left(\frac{a}{p}\right)$ – für ungerades a – zu berechnen, ist es nicht nötig, a in Primfaktoren zu zerlegen (Lerne später: Jacobi-Symbol)

Beweis von (R): "frei nach Eisenstein"

Für p, q wie oben setze $\zeta_p := e^{\frac{2\pi i}{p}}$, $\zeta_q := e^{\frac{2\pi i}{q}}$ (in $\mathbb{C}$)

$\left[\zeta_p^p = 1,\ \zeta_q^q = 1,\ \zeta_p \neq 1,\ \zeta_q \neq 1\right]$ und dann

(1) $[p,q] = \prod_{j=1}^{\frac{p-1}{2}} \prod_{k=1}^{q-1} (\zeta_p^j \zeta_q^k - \zeta_p^{-j} \zeta_q^{-k})$. Dann

$$[q,p]/[p,q] = \prod_{k=1}^{\frac{q-1}{2}} \prod_{j=\frac{p-1}{2}+1}^{p-1} (\zeta_q^k \zeta_p^j - \zeta_q^{-k}\zeta_p^{-j}) \Big/ \prod_{j=1}^{\frac{p-1}{2}} \prod_{k=\frac{q-1}{2}+1}^{q-1} (\zeta_p^j \zeta_q^k - \zeta_p^{-j}\zeta_q^{-k})$$

vgl. S. 185 jeweils für q

$$= \prod_{j=1}^{\frac{p-1}{2}} \prod_{k=1}^{\frac{q-1}{2}} (\zeta_q^k \zeta_p^{-j} - \zeta_q^{-k}\zeta_p^{j}) \Big/ \prod_{j=1}^{\frac{p-1}{2}} \prod_{k=1}^{\frac{q-1}{2}} (\zeta_p^j \zeta_q^{-k} - \zeta_p^{-j}\zeta_q^{k})$$

$$= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$ Also

(2) $[q,p] = [p,q](-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Somit

§ 2.2. $[p,q] = \left[\frac{q}{p}\right]$

$X^q - 1$ hat die q versch. Nst'n $1, \zeta_q, \zeta_q^2, \dots, \zeta_q^{q-1}$, also

$$X^q - 1 = (X-1)\prod_{k=1}^{q-1}(X-\zeta_q^k) = (X-1)\prod_{k=1}^{q-1}(X-\zeta_q^{2k})$$

Setze $\frac{y}{x}$ ein mit Variablen x, y:

$$\left(\frac{y}{x}\right)^q - 1 = \left(\frac{y}{x}-1\right)\prod_{k=1}^{q-1}\left(\frac{y}{x}-\zeta_q^{2k}\right), \text{ multipl. mit } x^q:$$

$$y^q - x^q = (y-x)\prod_{k=1}^{q-1}(y-x\zeta_q^{2k}) = (y-x)\underbrace{\prod_{k=1}^{q-1}\zeta_q^k}_{=1}\prod_{k=1}^{q-1}(y\zeta_q^{-k}-x\zeta_q^k)$$

$\Longrightarrow (-1)^{q-1}=1$

1, denn $1+2+\dots+q-1 = \frac{q-1}{2}q \equiv 0 \bmod q$

(3) $$\prod_{k=1}^{q-1}(x\zeta_q^k - y\zeta_q^{-k}) = \frac{x^q-y^q}{x-y}$$ (eine einfache algebraische Identität).

$$[p,q] \overset{(3)\ x\mapsto\zeta_p^j,\ y\mapsto\zeta_p^{-j}}{=} \prod_{j=1}^{\frac{p-1}{2}}\frac{\zeta_p^{jq}-\zeta_p^{-jq}}{\zeta_p^j-\zeta_p^{-j}} = \frac{\prod_{j=1}^{\frac{p-1}{2}}(\zeta_p^{jq}-\zeta_p^{-jq})}{\prod_{j=1}^{\frac{p-1}{2}}(\zeta_p^j-\zeta_p^{-j})}$$

Aber $$\prod_{j=1}^{\frac{p-1}{2}}(\zeta_p^{qj}-\zeta_p^{-qj}) \overset{\text{Gauß-Lemma}\ *)}{=} \left(\frac{q}{p}\right)\prod_{j=1}^{\frac{p-1}{2}}(\zeta_p^j-\zeta_p^{-j})$$

Es folgt

$$[p,q] = \left(\frac{q}{p}\right) \qquad \text{q.e.d.}$$

*) Für $j\in H = \{1,2,\dots,\frac{p-1}{2}\}$ ist $qj \equiv \varepsilon j' \bmod p$ mit eindeutigem $j'\in H$ und Vorzeichen $\varepsilon = \varepsilon(qj) = \pm 1$. Damit ist

$$\zeta_p^{qj}-\zeta_p^{-qj} = \zeta_p^{\varepsilon j'}-\zeta_p^{-\varepsilon j'} \overset{!}{=} \varepsilon(\zeta_p^{j'}-\zeta_p^{-j'}) \text{ mit } \varepsilon=\varepsilon(qj)$$

Produktbildung liefert $\prod_{j\in H}(\zeta_p^{qj}-\zeta_p^{-qj}) = \prod_{j\in H}\varepsilon(qj)\cdot\prod_{j\in H}(\zeta_p^j-\zeta_p^{-j})$

Nach Gauß ist aber $\prod_{j\in H}\varepsilon(qj) = \left(\frac{q}{p}\right)$.

Das Jacobisymbol: Aus algorithmischen Gründen vereinbaren wir

Def. $a, b \in \mathbb{Z} \setminus \{0\}$, b ungerade, $(a,b)=1$. Setze dann

$$\left(\frac{a}{b}\right)_J = \prod_{p \mid b} \left(\frac{a}{p}\right)^{w_p(b)} \qquad \text{Jacobisymbol}$$

Für $b=p$ Primzahl (nach Vor. $p \neq 2$) ist $\left(\frac{a}{p}\right)_J = \left(\frac{a}{p}\right)$

Fortsetzung des Legendresymbols. Lasse also Index J weg.

$\left(\frac{a}{b}\right) = 1$ oder -1 **beachte**: $\left(\frac{a}{-b}\right) = \left(\frac{a}{b}\right)$

Eigenschaften:

(1) $a \equiv a' \bmod b \Rightarrow \left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$

(2) $\left(\frac{a}{b}\right)\left(\frac{a'}{b}\right) = \left(\frac{aa'}{b}\right)$ und $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$

(3) $\left(\frac{x^2}{b}\right) = 1 = \left(\frac{a}{g^2}\right)$, $\left(\frac{ax^2}{b}\right) = \left(\frac{a}{b}\right) = \left(\frac{a}{bg^2}\right)$ $(x,b)=1$, $(g,a)=1$, g ungerade

(4) a quadr. Rest mod $b \Rightarrow \left(\frac{a}{b}\right) = 1$

[$c^2 \equiv a \bmod b \Rightarrow c^2 \equiv a \bmod p$ für alle $p \mid b \Rightarrow \left(\frac{a}{p}\right)=1$ für alle $p \mid b \Rightarrow \left(\frac{a}{b}\right)=1$]

⚠ Umkehrung von (4) gilt nicht:

$$\left(\frac{3}{133}\right) = \left(\frac{3}{7 \cdot 19}\right) = \left(\frac{3}{7}\right)\left(\frac{3}{19}\right) = -\left(\frac{7}{3}\right) \cdot -\left(\frac{19}{3}\right) = \left(\frac{7}{3}\right)\left(\frac{19}{3}\right) = \left(\frac{1}{3}\right)\left(\frac{1}{3}\right) = 1 \cdot 1 = 1$$

aber 3 kein quadr. Rest mod 133; sonst 3 quadr. Rest mod 7, doch $\left(\frac{3}{7}\right) = -1$.

Satz 1' (Reziprozitätsgesetz für das Jacobisymbol):

$b \in \mathbb{Z}$, b ungerade.

(E_1) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2} + \frac{\operatorname{sgn}(b)-1}{2}}$

für $b>0$ also: $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} = \begin{cases} 1 & \text{für } b \equiv 1 \bmod 4 \\ -1 & \text{für } b \equiv 3 \bmod 4 \end{cases}$

(E_2) $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} = \begin{cases} 1 & \text{für } b \equiv \pm 1 \bmod 8 \\ -1 & \text{für } b \equiv \pm 3 \bmod 8 \end{cases}$

(R) Ist auch a ungerade, und $(a,b)=1$, so

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2} + \frac{\operatorname{sgn}(a)-1}{2}\frac{\operatorname{sgn}(b)-1}{2}}, \text{ also}$$

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}, \text{ falls } b>0 \text{ oder } a>0$$

Bem. (E_1) in (R) enthalten: setze $a=-1$.

Beweis: Zuerst Lemma: x, y ungerade. Dann

(i) $\frac{xy-1}{2} \equiv \frac{x-1}{2} + \frac{y-1}{2} \bmod 2$ (ii) $\frac{(xy)^2-1}{8} \equiv \frac{x^2-1}{8} + \frac{y^2-1}{8} \bmod 2$

Denn: (i) $\Leftrightarrow$ $xy-1 \equiv x-1+y-1 \bmod 4 \Leftrightarrow (x-1)(y-1) \equiv 0 \bmod 4$ ✓

(ii) $\Leftrightarrow$ $(xy)^2-1 \equiv x^2-1+y^2-1 \bmod 16 \Leftrightarrow (x^2-1)(y^2-1) \equiv 0 \bmod 16$ ✓ □

Beweis von (E_1), (E_2): Die rechten Seiten verhalten sich multiplikativ in b aufgrund des Lemmas. Die linken sowieso. Es genügt also, folgende Fälle zu betrachten:

(1) $b = p$ Primzahl $(\neq 2)$ (2) $b = -1$

Fall (1) bekannt (1. u. 2. Ergänzungssatz für Legendresymbol).

Fall (2): Für $b=-1$ ist $\left(\frac{-1}{b}\right)=1$ nach Definition; rechte

$$\text{Seite} = (-1)^{\frac{-1-1}{2}+\frac{2a(-1)-1}{2}} = (-1)^{-1-1} = 1.$$

(E_2) für $b=-1$ trivial.

Bew. von (R): Sei $\psi(a,b)$ die linke Seite, $\varepsilon(a,b)$ die rechte.
Beide sind multiplikativ bzgl. a und b (einzeln).
Für ε nach Lemma 1. Außerdem symmetrisch in a und b.

Es genügt also zu zeigen:

(α) $\psi(p,q)=\varepsilon(p,q)$ für ungerade Primzahlen p,q mit $p\neq q$

(β) $\psi(p,-1)=\varepsilon(p,-1)$

(γ) $\psi(-1,-1)=\varepsilon(-1,-1)$

(γ): $\varepsilon(-1,-1)=1=\psi(-1,-1)$

(β): $\varepsilon(p,-1)=(-1)^{\frac{p-1}{2}}=\left(\frac{-1}{p}\right)=\psi(p,-1)$

(α) ist das ursprüngliche Reziprozitätsgesetz (Satz 1).

q.e.d.

Beispiele: a) $\left(\frac{219}{383}\right)=-\left(\frac{383}{219}\right)=-\left(\frac{164}{219}\right)=-\left(\frac{4\cdot 41}{219}\right)=-\left(\frac{41}{219}\right)=-\left(\frac{219}{41}\right)=$

$-\left(\frac{14}{41}\right)=-\left(\frac{2}{41}\right)\left(\frac{7}{41}\right)=-\left(\frac{7}{41}\right)=-\left(\frac{41}{7}\right)=-\left(\frac{-1}{7}\right)=+1=1$, also ist

219 ein QR mod 383 (denn 383 ist prim!)

b) $\left(\frac{5}{1363}\right)=\left(\frac{1363}{5}\right)=\left(\frac{3}{5}\right)=-1$, also ist 5 ein NQR mod 1363 (obwohl $1363=29\cdot 47$ nicht prim ist).

c) wie $\left(\frac{5}{219}\right)=\left(\frac{219}{5}\right)=\left(\frac{4}{5}\right)=1$, demnach ist 5 ein NQR mod 219

Korollar: Sei $a \in \mathbb{N}$ gegeben. Für alle ungeraden $b \in \mathbb{Z}$ hängt $\left(\frac{a}{b}\right)$ von b nur modulo $4a$ ab, im Falle $a \equiv 1 \bmod 4$ sogar nur modulo a. (Präzisiert: dabei sei b stets prim zu a).

Bew: 1) Fall: a ungerade. Seien $b, b' \in \mathbb{Z}$ mit $b \equiv b' \bmod a$; dabei b, b' ungerade und prim zu a. Nach Satz 1' dann

$a>0$ $\quad \left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)(-1)^{\frac{a-1}{2}\frac{b-1}{2}}$, $\left(\frac{a}{b'}\right) = \left(\frac{b'}{a}\right)(-1)^{\frac{a-1}{2}\frac{b'-1}{2}} = \left(\frac{b}{a}\right)(-1)^{\frac{a-1}{2}\frac{b'-1}{2}}$

Für $a \equiv 1 \bmod 4$ folgt $\left(\frac{a}{b}\right) = \left(\frac{a}{b'}\right)$.

Für $a \equiv 3 \bmod 4$ folgt $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)(-1)^{\frac{b-1}{2}}$, $\left(\frac{a}{b'}\right) = \left(\frac{b}{a}\right)(-1)^{\frac{b'-1}{2}}$

Ist nun $b \equiv b' \bmod 4a$, so $b \equiv b' \bmod 4$, und es folgt $\left(\frac{a}{b}\right) = \left(\frac{a}{b'}\right)$

2) Fall: a gerade. o.E. a quadratfrei, also o.E.

$a = 2a_1$ mit a_1 ungerade. Gelte $b \equiv b' \bmod 4a = 8a_1$.

Es folgt

$$\left(\frac{a}{b'}\right) = \left(\frac{2}{b'}\right)\left(\frac{a_1}{b'}\right) \overset{Ez}{=} \left(\frac{2}{b}\right)\left(\frac{a_1}{b'}\right) \overset{1)}{=} \left(\frac{2}{b}\right)\left(\frac{a_1}{b}\right) = \left(\frac{a}{b}\right).$$

Bem. Analoges gilt auch für $a \in \mathbb{Z} \setminus \{0\}$, wenn man für $\left(\frac{a}{b}\right)$ nur b mit $b>0$ (also nur $b \in \mathbb{N}$) zuläßt.

Aufgabe: Bestimme alle Primzahlen p, für die $a=7$ ein QR mod p ist, d.h. alle Primzahlen p $(\neq 2, 7)$ mit

$$\left(\frac{7}{p}\right) = 1$$

Lösung: Es ist $4a = 28$. Betrachte die Abb.

$\chi: (\mathbb{Z}/28)^\times \longrightarrow \{+1,-1\}$ mit $\chi(b \bmod 28) = \left(\frac{7}{b}\right)$

Wegen des Korollars ist χ wohldefiniert! Und ein Homomorphismus. Trivialerweise gilt

(1) $$\left(\frac{7}{-b}\right) = \left(\frac{7}{b}\right)$$

Ferner $\left(\frac{7}{5}\right) \cdot \left(\frac{2}{5}\right) = -1$ (und daher $\left(\frac{7}{b}\right) = 1 \Leftrightarrow \left(\frac{7}{5b}\right) = -1$).

Es folgt

(2) $$\#\operatorname{Ker}\chi = \frac{\varphi(28)}{2} = \frac{\varphi(4)\varphi(7)}{2} = \frac{2\cdot 6}{2} = 6$$

Mit Blick auf (1) wird $\operatorname{Ker}\chi$ also mod 28 repräsentiert durch 6 Zahlen der Gestalt $\pm b$ mit $|b|<14$.

Wegen $\left(\frac{7}{1}\right)=1$, $\left(\frac{7}{3}\right)=1$, $\left(\frac{7}{9}\right)=\left(\frac{7}{3^2}\right)=1$ sind dies genau die Zahlen

(3) $$\pm 1, \pm 3, \pm 9$$

<u>Antwort:</u> Die gesuchten p sind genau die p, die modulo 28 kongruent sind zu einer der 6 Zahlen

$\pm 1, \pm 3, \pm 9$ (bzw. zu 1, 3, 9, 19, 25, 27) □

Aus Bem. zu Korolla (S. 116) folgt:
Die Primzahlen p mit $\left(\frac{-3}{p}\right) = 1$ sind (wegen $-3 \equiv 1 \bmod 4$) genau die p mit $p \equiv 1 \bmod 3$.