REMARKS ON QUADRATIC RECIPROCITY
(INSPIRED BY GAUSS' "DISQUISITIONES ARITHMETICAE")

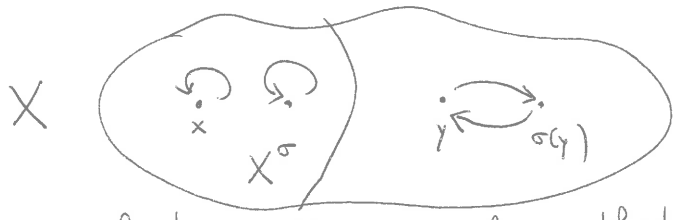
Variations on $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ via Wilson's thm

(1) $$\left(\frac{-1}{p}\right) \overset{\text{Wilson's thm}}{=\!=\!=} \left(\frac{(p-1)!}{p}\right) = \prod_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) = 1^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}}$$

---

(2) The standard pf of Wilson's thm uses the involution $\sigma: x \longmapsto x^{-1}$ on $\mathbb{F}_p^\times$ with fixed points $\sigma(x) = x \iff x = \pm 1$.

In general, if $\sigma: X \longrightarrow X$ is an involution on a set X (i.e., a map satisfying $\sigma \circ \sigma = id$), then the orbits under the action of σ are either fixed points $x = \sigma(x)$, or pairs of elements mutually exchanged by σ:



If X is finite, this implies that the set of fixed points $X^\sigma = \{x \in X \mid \sigma(x) = x\}$ satisfies

$$\boxed{|X^\sigma| \equiv |X| \pmod 2} \quad (*)$$

Ex: $\sigma: \mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times$ $(p \neq 2)$. This involution preserves $\mathbb{F}_p^{\times 2}$; its fixed points there are

$$(\mathbb{F}_p^{\times 2})^\sigma = \mathbb{F}_p^{\times 2} \cap (\mathbb{F}_p^\times)^\sigma = \mathbb{F}_p^{\times 2} \cap \{\pm 1\} = \begin{cases} \{\pm 1\}, & -1 \in \mathbb{F}_p^{\times 2} \\ \{1\}, & -1 \notin \mathbb{F}_p^{\times 2}. \end{cases}$$

In other words,

$$(-1)^{|(\mathbb{F}_p^{\times 2})^\sigma|} = \left(\frac{-1}{p}\right).$$

Combined with $(*)$, this gives

$$\left(\frac{-1}{p}\right) = (-1)^{|(\mathbb{F}_p^{\times 2})^\sigma|} \overset{(*)}{=} (-1)^{|\mathbb{F}_p^{\times 2}|} = (-1)^{\frac{p-1}{2}}.$$

---

(3) This argument can be iterated. Assume that $-1 \in \mathbb{F}_p^{\times 2}$, which is equivalent to $p \equiv 1\ [4]$, and fix $a \in \mathbb{F}_p^\times$ such that $a^2 = -1$. The equation $X^4 - 1 = 0$ has at most 4 solutions in $\mathbb{F}_p$, which means that they are precisely $\pm 1, \pm a$.

The fibres of the surjective map $\mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^{\times 4}$, $x \longmapsto x^4$ are of the form $\{\pm x, \pm ax\}$; therefore $|\mathbb{F}_p^{\times 4}| = \frac{p-1}{4}$.

Again, the involution $\sigma : x \longmapsto x^{-1}$ preserves $\mathbb{F}_p^{\times 4}$, and its fixed points are

$$(\mathbb{F}_p^{\times 4})^\sigma = \mathbb{F}_p^{\times 4} \cap \{\pm 1\} = \begin{cases} \{\pm 1\} & \text{if } -1 \in \mathbb{F}_p^{\times 4} \\ \{+1\} & \text{if } -1 \notin \mathbb{F}_p^{\times 4}. \end{cases}$$

As $$|(\mathbb{F}_p^{\times 4})^\sigma| \equiv |\mathbb{F}_p^{\times 4}| = \frac{p-1}{4} \pmod 2$$

by (*), it follows that

$$-1 \in \mathbb{F}_p^{\times 4} \iff p \equiv 1 \pmod 8.$$

---

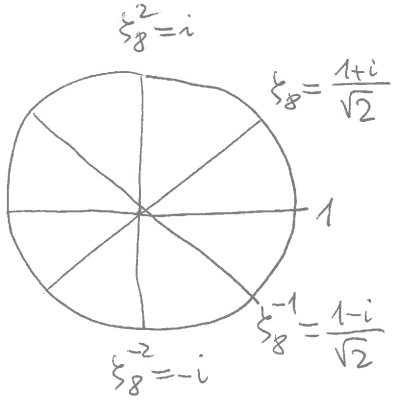
(4) Exercise. Show by induction that

$$\forall\, k \geq 0 \qquad -1 \in (\mathbb{F}_p^\times)^{2^k} \iff p \equiv 1 \pmod{2^{k+1}}.$$

---

(5) If $p \equiv 1\ [2^{k+1}]$ $(k \geq 0)$, any solution of $a^{2^k} = -1$ in $\mathbb{F}_p$ (there are 2^k of them) behaves like $e^{\pm i/2^k} = \zeta_{2^{k+1}}$.

For example, if $k = 2$ and $a^4 = -1$, then



$$\zeta_8 = \frac{1+i}{\sqrt{2}}, \quad \zeta_8^{-1} = \frac{1-i}{\sqrt{2}}, \quad \zeta_8 - \zeta_8^{-1} = i\sqrt{2},$$

$$\boxed{(\zeta_8 - \zeta_8^{-1})^2 = -2.}$$

In $\mathbb{F}_p$, we have an analogous relation

$$(a - a^{-1})^2 = \frac{a^4 + 1 - 2a^2}{a^2} = -2.$$

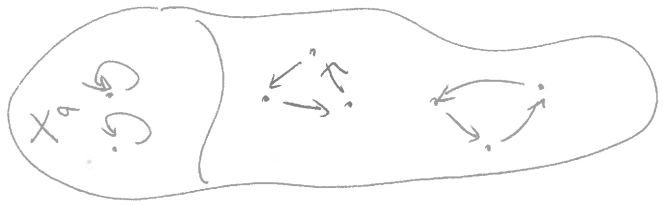
In particular, $\left(\frac{-2}{p}\right) = 1$ if $p \equiv 1\ [8]$.

$\left(\Longrightarrow \left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{-1}{p}\right) = 1 \quad \text{for } p \equiv 1\ [8]\right)$.

(6) A slightly more general version of (*) states that, if $\sigma: X \longrightarrow X$ satisfies $\sigma^p = \underbrace{\sigma \circ \dots \circ \sigma}_{p \text{ times}} = id$ for a prime number p,

then $$\boxed{|X^\sigma| \equiv |X| \pmod{p} \qquad (**)}.$$

This follows again from the fact that orbits of σ acting on X are either fixed points or p-cycles (exercise: $\sigma(x), \sigma^2(x), \dots, \sigma^p(x) = x$ are distinct if $\sigma(x) \neq x$):



$(p = 3)$

More generally, if a group G of order p^n $(n \geq 0)$ acts on a finite set X, then the set of fixed points $$X^G = \{x \in X \mid \forall g \in G \quad g(x) = x\}.$$

satisfies

$$|X^G| \equiv |X| \pmod{p}.$$

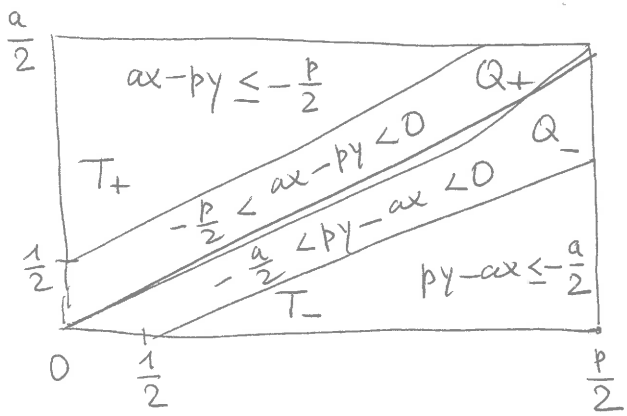
See (??) for a pf of QRL based on (**).

QRL via Gauss' Lemma

Gauss' Lemma: if $p \nmid a$, then $\left(\frac{a}{p}\right) = (-1)^k$, where

$$k = \left| \left\{ (x,y) \in \mathbb{Z}^2 \;\middle|\; 0 < x < \frac{p}{2},\ -\frac{p}{2} < ax - py < 0 \right\} \right|.$$

these inequalities imply that $y < \frac{ax}{p} + \frac{1}{2}$ $\left(< \frac{a+1}{2} \text{ if } a > 0 \right)$.
If $2 \nmid a$, then $y \leq \frac{a}{2}$ and we can draw the following picture



The rectangle

$$R = \left\{ 0 \leq x \leq \frac{p}{2},\ 0 \leq y \leq \frac{a}{2} \right\}$$ is a disjoint union of two triangles T_+, T_- and two quadrilaterals Q_+, Q_-.

If $a = q \neq p$ is a prime, then

$$\left(\frac{q}{p}\right) = (-1)^k, \qquad k = |Q_+ \cap \mathbb{Z}^2|$$

$$\left(\frac{p}{q}\right) = (-1)^\ell, \qquad \ell = |Q_- \cap \mathbb{Z}^2|.$$

the total number of lattice points in R is

$$\left| (Q_+ \cup Q_- \cup T_+ \cup T_-) \cap \mathbb{Z}^2 \right| = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

there is a bijection between lattice points in T_+ and T_-, given by

$$T_+ \cap \mathbb{Z}^2 \longleftrightarrow T_- \cap \mathbb{Z}^2$$

$$(x, y) \longmapsto \left(\frac{p+1}{2} - x,\ \frac{q+1}{2} - y \right).$$

Putting all of this together, we obtain

$$k + \ell = |R \cap \mathbb{Z}^2| - |T_+ \cap \mathbb{Z}^2| - |T_- \cap \mathbb{Z}^2| \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2$$

and

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{k+\ell} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Descent and QRL

The statement of the QRL

$QRL(p,q) = QRL(q,p)$: $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$, $\quad q^* = (-1)^{\frac{q-1}{2}} q = \left(\frac{-1}{q}\right) q$

is a conjunction of two implications:

$$\left(\frac{p}{q}\right) = -1 \Rightarrow \left(\frac{q^*}{p}\right) = -1$$

and its converse

$$\left(\frac{p}{q}\right) = -1 \Leftarrow \left(\frac{q^*}{p}\right) = -1 .$$

For fixed q, the first implication can be proved by descent, provided it is known to be true for all $p < q$ (if $q^* < 0$, then $p \leq \frac{q+1}{2}$ suffices). The argument is a refinement of the trick used in the proof of the fact that there are infinitely many primes $p \equiv 3\ [4]$, namely, that a positive integer of the form $4k+3$ is always divisible by a prime of the same form.

This result can be combined with another descent argument to show that (for fixed q) $QRL(p,q)$ holds whenever $\left(\frac{p}{q}\right) = -1$ or $\left(\frac{-1}{p}\right) = -1$, provided it holds for such p with $p < q$.

The same method also determines the values of $\left(\frac{2}{p}\right)$ if $p \not\equiv 1\ [8]$.

We are going to illustrate this method by looking at the simplest case $q = 3$. After that we pass to the general case.

Example 1: $\boxed{p \equiv -1\ [3] \Rightarrow \left(\frac{-3}{p}\right) = -1}$

Assume that $p \equiv -1\ [3]$ and $\left(\frac{-3}{p}\right) = 1$. We are going to perform

Descent for $x^2 \equiv -3\ [p]$:

By assumption, there exists $a \in \mathbb{Z}$ such that $a^2 \equiv -3\ [p]$. After replacing a by $\pm a + kp$ we can assume that

$$a^2 = -3 + pb, \quad 0 < a < \frac{p}{2}, \quad 2 \mid a.$$

These conditions imply that $2 \nmid b$ and $0 < b < \frac{a^2+3}{p} \leq \frac{\left(\frac{p}{2}-1\right)^2+3}{p} < p$.

Case (I): $\boxed{3 \nmid a} \Rightarrow (a, b) = 1 \Rightarrow \forall$ prime $p' \mid b$ $a^2 \equiv -3\ [p']$ $\left(\Rightarrow \left(\frac{-3}{p'}\right) = 1\right)$ and $p' \leq b < p$.

$\Downarrow$

$pb \equiv a^2 \equiv 1\ [3] \Rightarrow b \equiv -1\ [3] \Rightarrow \exists$ prime $p' \mid b$ $(\Rightarrow p' \neq 2)$ such that $p' \equiv -1\ [3]$.

Case (II): $\boxed{3 \mid a}$ $a = 3^m A$, $m \geq 1$, $b = 3B$, $3 \nmid AB$,

$3^{2m-1} A^2 = -1 + pB \Rightarrow \forall$ prime $p' \mid B$ ($(a, B) = 1$ and) $a^2 \equiv -3\ [p']$

$\Downarrow$

$\left(\left(\frac{-3}{p'}\right) = 1\right)$ and $p' \leq B < p$.

Again, $pB \equiv 1\ [3] \Rightarrow B \equiv -1\ [3] \Rightarrow \exists$ prime $p' \mid B$ $(\Rightarrow p' \neq 2)$ such that $p' \equiv -1\ [3]$.

Summary of descent: if $p \equiv -1\ [3]$ and $\left(\frac{-3}{p}\right) = 1$ then there exists $p' < p$ with the same property.

Conclusion: $\boxed{\forall p\ p \equiv -1\ [3] \Rightarrow \left(\frac{-3}{p}\right) = -1}$ $\left(\frac{p}{3}\right) = -1$

Equivalently: $\boxed{p \not\equiv 1\ [3] \Rightarrow \left(\frac{-3}{p}\right) = -1}$

Consequences: $p \equiv 5\ [12] \Rightarrow \left(\frac{3}{p}\right) = \left(\frac{-3}{p}\right)\left(\frac{-1}{p}\right) = -1$.

$p \equiv 11\ [12] \Rightarrow \left(\frac{3}{p}\right) = 1$.

the next step is to leverage this result to ~~obtain~~ determine the value of $\left(\frac{3}{p}\right)$ (and thus of $\left(\frac{-3}{p}\right)$) if $p \equiv 7\ [12]$.

Example 2: $\boxed{p \equiv 7\,[12] \Longrightarrow \left(\frac{3}{p}\right) = -1}$

Assume that $p \equiv 7\,[12]$, $\left(\frac{3}{p}\right) = 1$. We are going to perform

Descent for $x^2 \equiv 3\,[p]$ As in Example 1, there exist $a, b \in \mathbb{Z}$ such that

$a^2 = 3 + pb$, $0 < a < p$, $2 \mid a \Longrightarrow 2 \nmid b$, $1 - 3 \leq pb < a^2 < p^2$

$\Longrightarrow 0 < b < p$.

Case (I): $3 \times a$ $pb \equiv a^2 \equiv 1\,[3]$, $pb \equiv 0 - 3 \equiv 1\,[4] \Longrightarrow pb \equiv 1\,[12]$

$\Longrightarrow b \equiv 7\,[12]$. Again, $\forall$ prime $p' \mid b$ $(\Rightarrow p' \neq 2, 3)$ $\left(\frac{3}{p'}\right) = 1$

$p' \leq b < p$. $\Longrightarrow p' \not\equiv 5\,[12]$, by Cor. Ex. 1.

On the other hand, $b \equiv 7\,[12]$ implies that $\exists$ prime $p' \mid b$ such that $p' \not\equiv \pm 1\,[12]$; therefore $p' \not\equiv \pm 1, 5\,[12] \Longrightarrow p' \equiv 7\,[12]$.

Case (II). $3 \mid a$ Again, $a = 3^m A$, $m \geq 1$, $b = 3B$, $3 \times AB$ $\quad p' \not\equiv 5\,[12]$.

$3^{2m-1} A^2 = 1 + pB \Longrightarrow (a, B) = 1$ and $\forall p' \mid B \quad a^2 \equiv 3\,[p'] \Longrightarrow \left(\frac{3}{p'}\right) = 1$.

As $pB \equiv -1\,[3]$ and $pB \equiv -1\,[4]$, we have $B \equiv -7 \equiv 5\,[12]$.

As in Case (I), $\exists$ prime $p' \mid B$ $p' \not\equiv \pm 1\,[12] \Longrightarrow p' \not\equiv \pm 1, 5\,[12]$

and so $p' \equiv 7\,[12]$.

Summary of descent: if $p \equiv 7\,[12]$ and $\left(\frac{3}{p}\right) = 1$ then there exists $p' < p$ with the same property.

Conclusion: $\boxed{\forall p \quad p \equiv 7\,[12] \Longrightarrow \left(\frac{3}{p}\right) = -1.}$

Results ~~Consequences~~ of Examples 1 and 2: $\boxed{\begin{array}{l} p \equiv \pm 5\,[12] \Longrightarrow \left(\frac{3}{p}\right) = -1 \\ p \equiv -1\,[12] \Longrightarrow \left(\frac{3}{p}\right) = 1 \end{array}}$

Exercise: (1) $p \equiv \pm 2\,[5] \Longrightarrow \left(\frac{5}{p}\right) = -1$. [Hint: descent for $x^2 \equiv 5\,[p]$ combined with the fact that a positive integer of the form $5k \pm 2$ is divisible by a prime of the form $5\ell + 2$ or $5\ell' - 2$.]

(2) Determine the values of $\left(\frac{\pm 5}{p}\right)$ for all $p \neq 1, 9\,[20]$ $(p \neq 2, 5)$

[Hint: combine the result of (1) with descent for $x^2 \equiv -5\,[p]$, as in Example 2, 2'.]

$\left(\frac{3}{p}\right) = -1$ revisited and simplified

Example 2′ (improvement of Example 2 above):

$$\underbrace{p \not\equiv \pm 1 \ [12]}_{p \equiv 5, 7 \ [12]} \Rightarrow \left(\frac{3}{p}\right) = -1$$

Assume that $p \not\equiv \pm 1 \ [12]$, $\left(\frac{3}{p}\right) = 1$. We are going to perform

Descent for $x^2 \equiv 3 \ [p]$ As in Example 1, there exist $a, b \in \mathbb{Z}$ such that

$a^2 = 3 + pb$, $0 < a < p$, $2 \mid a \Rightarrow \underline{2 \nmid b}$, $1 - 3 \le pb < a^2 < p^2 \Rightarrow \underline{0 < b < p}$.

Case (I): $\boxed{3 \nmid a}$ In this case $(6a, b) = 1$. For each prime $p' \mid b$ the congruence $a^2 \equiv 3 \ [p']$ yields $\underline{\left(\frac{3}{p'}\right) = 1}$. On the other hand, $pb \equiv 0 - 3 \equiv 1 \ [4]$ and $pb \equiv a^2 \equiv 1 \ [3]$, hence $pb \equiv 1 \ [12]$ and $b \not\equiv \pm 1 \ [12]$. This implies that $\exists$ prime $\underline{p' \mid b}$ such that $\underline{p' \not\equiv \pm 1 \ [12]}$. Of course, $p' \le b < p$.

Case (II): $\boxed{3 \mid a}$ Again, $a = 3^m A$, $m \ge 1$, $b = 3B$, $3 \nmid AB$,

$3^{2m-1} A^2 = 1 + pB \Rightarrow (2a, B) = 1$ and $\forall$ prime $p' \mid b$ $a^2 \equiv 3 \ [p']$, hence $\underline{\left(\frac{3}{p'}\right) = 1}$. On the other hand, $pB \equiv -1 \ [4]$ and $pB \equiv -1 \ [3]$, hence $pB \equiv -1 \ [12]$ and $B \not\equiv \pm 1 \ [12]$. As in Case (I), there exists a prime $p' \mid B$ ($\Rightarrow p' < p$) such that $p' \not\equiv \pm 1 \ [12]$

Summary of descent: if $p \not\equiv \pm 1 \ [12]$ and $\left(\frac{3}{p}\right) = 1$, then there exists $p' < p$ with the same property.

Conclusion:

$$\forall p \quad \underbrace{p \not\equiv \pm 1 \ [12]}_{p \equiv 5, 7 \ [12]} \Rightarrow \left(\frac{3}{p}\right) = -1.$$

Therefore $p \equiv 5 \ [12] \Rightarrow \left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = -1$

(already proved in Example 1)

$p \equiv 7 \ [12] \Rightarrow \left(\frac{-3}{p}\right) = 1$ (new result)

Example 3: $p \equiv \pm 5 \ [8] \Rightarrow \left(\frac{2}{p}\right) = -1$

Note: $p \equiv \pm 5 \ [8] \Rightarrow p \not\equiv \pm 1 \ [8]$

Assume that $p \equiv \pm 5 [8]$, $\left(\frac{2}{p}\right) = 1$.

Descent for $x^2 \equiv 2 [p]$: there exist $a, b \in \mathbb{Z}$ such that $a^2 = 2 + pb$, $0 < a < p$, $2 \nmid a$; thus $2 \nmid b$ and $1 - 2 \leq pb < a^2 < p^2$

$\Rightarrow 0 < b < p$. As $2 \nmid a$, we have $pb \equiv a^2 - 2 \equiv 1 - 2 \equiv -1 [8] \Rightarrow$

$b \equiv \mp 5 [8]$. It follows that there exists a prime $p' | b$ such that $p' \not\equiv \pm 1 \ [8] \Rightarrow p' \equiv \pm 5 [8]$. Then $p' \leq b < p$ and $a^2 \equiv 2 \ [p']$, hence $\left(\frac{2}{p'}\right) = 1$.

Summary of descent: if $p \equiv \pm 5 [8]$ and $\left(\frac{2}{p}\right) = 1$ then there exists $p' < p$ with the same property.

Conclusion: $\forall p \quad p \equiv \pm 5 [8] \Rightarrow \left(\frac{2}{p}\right) = -1$

Cor. $p \equiv 5 [8] \Rightarrow \left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right) = -1$

$p \equiv -5 [8] \Rightarrow \left(\frac{-2}{p}\right) = 1$.

Example 4: $p \equiv -1 [8] \Rightarrow \left(\frac{-2}{p}\right) = -1$

Assume that $p \equiv -1 [8]$, $\left(\frac{-2}{p}\right) = 1$.

Descent for $x^2 \equiv -2 [p]$ Again, $a^2 \equiv -2 + pb$, $0 < a < p$, $2 \nmid a \Rightarrow$ $2 \nmid b$, $0 < pb \leq (p-1)^2 + 2 \Rightarrow 0 < b < p$. Moreover, $pb \equiv a^2 + 2 \equiv 3 [8]$ and $b \equiv 5 [8]$. For each prime $p' | b$ ($\Rightarrow p' \nmid 2a$) $a^2 \equiv -2 [p']$ implies that $\left(\frac{-2}{p'}\right) = 1 \overset{\text{Cor. Ex. 3}}{\Longrightarrow} p' \not\equiv 5 [8] \Rightarrow p' \equiv \pm 1, 3 [8]$

As $b \equiv 5 [8]$, $\exists$ prime $p' | b$ such that $p' \not\equiv 1, 3 [8] \Rightarrow p' \equiv -1 [8]$.

Summary of descent: if $p \equiv -1 [8]$ and $\left(\frac{-2}{p}\right) = 1$ then there exists $p' < p$ with the same property.

Conclusion: $\forall p \quad p \equiv -1 [8] \quad \left(\frac{-2}{p}\right) = -1$ $\left(\Rightarrow \left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{-1}{p}\right) = 1\right)$

$\left(\frac{-2}{p}\right)=-1$ revisited and simplified

Example 4' (improvement of Example 4 above):

$$p \not\equiv 1, 3 \ [8] \Longrightarrow \left(\frac{-2}{p}\right)=-1$$

Descent for $x^2 \equiv -2 \ [p]$ Assume that $p \not\equiv 1,3 \ [8]$, $\left(\frac{-2}{p}\right)=1$.

As above, there exist integers $a, b \in \mathbb{Z}$ such that

$a^2=-2+pb$, $0<a<p$, $2 \nmid a$ $\Longrightarrow$ $2 \nmid b$, $0<b \leq \frac{(p-1)^2+2}{p}<p$.

For each prime $p' \mid b$ we have $p' \nmid 2a$ and $a^2 \equiv -2 \ [p']$, hence $\left(\frac{-2}{p'}\right)=1$. Moreover, $pb \equiv a^2+2 \equiv 3 \ [8]$, which implies that $b \not\equiv 1,3 \ [8]$. For such b there is always a prime $p' \mid b$ satisfying $p' \not\equiv 1,3 \ [8]$ (since $3 \cdot 3 \equiv 1 \ [8]$).

Summary of descent: if $p \not\equiv 1,3 \ [8]$ and $\left(\frac{-2}{p}\right)=1$ then there exists $p'<p$ with the same property.

Conclusion: $$\forall \ p \not\equiv 1,3 \ [8] \quad \left(\frac{-2}{p}\right)=-1$$

Consequences: $p \equiv 5 \ [8] \Longrightarrow \left(\frac{-2}{p}\right)=-1, \ \left(\frac{2}{p}\right)=\left(\frac{-2}{p}\right)\left(\frac{-1}{p}\right)=-1$

$p \equiv 7 \ [8] \Longrightarrow \left(\frac{-2}{p}\right)=-1, \ \left(\frac{2}{p}\right)=1$

Examples 3+4' determine the values of $\left(\frac{\pm 2}{p}\right)$ if $p \not\equiv 1 \ [8]$.

the case $p \equiv 1 \ [8]$ was treated earlier directly, by another method ($(\xi_8-\xi_8^{-1})^2=-2$).

Question: what can one deduce from descent for $x^2 \equiv -1 \ [p]$?

(Answer: the "easy" implication $p \not\equiv 1 \ [4] \Longrightarrow \left(\frac{-1}{p}\right)=-1$)

Descent for $x^2 \equiv q^* [p]$

We are now going to treat the general implication

$$A(p,q): \quad \left(\frac{p}{q}\right) = -1 \implies \left(\frac{q^*}{p}\right) = -1$$

(or, equivalently, $\left(\frac{q^*}{p}\right) = 1 \implies \left(\frac{p}{q}\right) = 1$). This statement amounts to saying that $QRL(p,q)$ holds in the case $\left(\frac{p}{q}\right) = -1$ (equivalently, in the case $\left(\frac{q^*}{p}\right) = 1$).

Recall that

$$q^* = \left(\frac{-1}{q}\right) q = (-1)^{\frac{q-1}{2}} q = \begin{cases} q, & q \equiv 1 \,[4] \\ -q, & q \equiv -1 \,[4]. \end{cases}$$

Descent Lemma for $x^2 \equiv q^* [p]$:

If $A(p,q)$ is false and $\begin{cases} p > q & \text{if } q^* > 0 \\ p > \frac{q+1}{2} & \text{if } q^* < 0 \end{cases}$, then $\exists\, p' < p$ such that $A(p',q)$ is false.

Corollary. Fix q. If $QRL(p,q)$ holds for all $\begin{cases} p < q & \text{if } q^* > 0 \\ p \le \frac{q+1}{2} & \text{if } q^* < 0 \end{cases}$ satisfying $\left(\frac{p}{q}\right) = -1$, then it holds for all p satisfying $\left(\frac{p}{q}\right) = -1$.

Examples: (1) $q = 3$: $\forall p$ $\left(\frac{p}{3}\right) = -1 \implies \left(\frac{-3}{p}\right) = -1$ (Example 1 above).

(2) $q = 5$: ~~(3)~~ $QRL(3,5)$ holds by (1), hence

$$\forall p \quad \left(\frac{p}{5}\right) = -1 \implies \left(\frac{5}{p}\right) = -1 \quad \text{(Exercise 3 (1) above)}$$

(3) $q = 7$: $QRL(3,7)$ holds, since $\left(\frac{7}{3}\right) = 1 = -\left(\frac{3}{7}\right)$; therefore

$$\forall p \quad \underbrace{\left(\frac{p}{7}\right) = -1}_{p \equiv -1, -2, -4 \,[7]} \implies \left(\frac{-7}{p}\right) = -1$$

Pf of Descent Lemma. Assume that $\left(\frac{p}{q}\right)=-1$ and $\left(\frac{q^*}{p}\right)=1$.

By assumption, there exists $a\in\mathbb{Z}$ such that $a^2\equiv q^*\ [p]$. After replacing a by $\pm a+kp$ we can assume that $a^2=q^*+pb$, $0<a<p$, $2\mid a$. The integer b satisfies $2\nmid b$.

Assume, in addition, that $\begin{cases} p>q & \text{if } q^*>0 \\ p>\frac{q+1}{2} & \text{if } q^*<0 \end{cases}$.

If $q^*>0$, then $-p<-q<a^2-q=pb<a^2<p^2$, hence $0<b<p$.

If $q^*<0$, then $0<pb=a^2+q<(p-1)^2+(2p-1)=p^2\Rightarrow 0<b<p$.

Case (I): $q\nmid a$ In this case $(2aq,b)=1$. As $pb\equiv a^2\ [q]$, we have $\left(\frac{b}{q}\right)=\left(\frac{p}{q}\right)=-1$,

(and $\forall$ prime $p'\mid b$ $a^2\equiv q^*\ [p']\Rightarrow\left(\frac{q^*}{p'}\right)=1$.)

which implies that there exists a prime $p'\mid b$ such that $\left(\frac{p'}{q}\right)=-1$. It also satisfies $\left(\frac{q^*}{p'}\right)=1$ (and $p'\le b<p$).

$A(p',q)$ is false

Case (II): $q\mid a$ In this case $a=q^mA$, $m\ge 1$, $b=qB$, $q\nmid AB$.

the equality $q^{2m-1}A^2=(q^*/q)+pb'$ implies that $(2a,b')=1$ and that $\forall$ prime $p'\mid b'$ $(\Rightarrow p'\neq 2,q;\ p'\nmid a)$ $a^2\equiv q^*\ [p']$, hence $\left(\frac{q^*}{p'}\right)=1$. On the other hand, $pb'\equiv(-q^*/q)\ [q]$ and $\left(\frac{pb'}{q}\right)=\left(\frac{-q^*/q}{q}\right)=1$. therefore $\left(\frac{b'}{q}\right)=\left(\frac{p}{q}\right)=-1$, which means that there exists a prime $p'\mid b'$ satisfying $\left(\frac{p'}{q}\right)=-1$. Again, $A(p',q)$ is false and $p'\le b'<b<p$.

~~this result will be used as an input into the following descent argument.~~

Descent for $x^2 \equiv -q^* [p]$

In the previous section we considered QRL(p,q) in the special case when $\left(\frac{q^*}{p}\right) = 1$. We are now going to treat the case $\left(\frac{-q^*}{p}\right) = 1$, when QRL$(p,q)$ says that

$$\left(\frac{-q^*}{p}\right) = 1 \Rightarrow \left(\frac{p}{q}\right) = \left(\frac{-1}{p}\right).$$

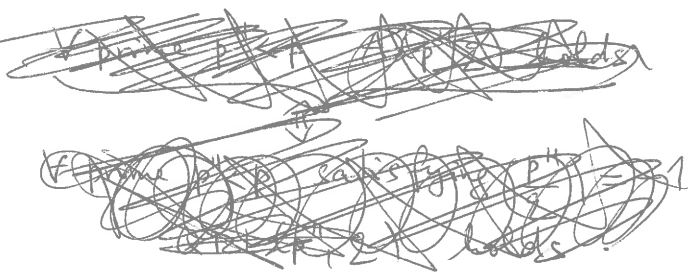
Equivalently, we may consider this as the following special case

$$\left(\frac{p}{q}\right) = -\left(\frac{-1}{p}\right) \Rightarrow \left(\frac{-q^*}{p}\right) = -1$$

of QRL(p,q).

Descent Lemma for $x^2 \equiv -q^* [p]$: Fix q and assume that p is a prime such that

(*) $\left(\frac{-q^*}{p}\right) = 1$, $\left(\frac{p}{q}\right) \neq \left(\frac{-1}{p}\right)$ and



If $\begin{cases} p > \frac{q+1}{2} & \text{if } q^* > 0 \\ p > q & \text{if } q^* < 0 \end{cases}$, then $\exists$ prime $p' < p$ for which (*) holds.

Pf. As before, there exist $a, b \in \mathbb{Z}$ such that

$a^2 = -q^* + bp$, $0 < a < p$, $2 \nmid a$; then $2 \nmid b$ and $q^*/p < b \leq (a^2 + q^*)/p$.

If $q^* > 0$, then $0 < b \leq \frac{(p-1)^2 + q}{p} \leq \frac{(p-1)^2 + (2p-1)}{p} = p$.

If $q^* < 0$, then $-p < -q < bp < a^2 < p^2$, hence $0 < b < p$.

Case (I): $q \nmid a$ Again, $(2aq, b) = 1$ in this case, and

$\forall$ prime $p' \mid b$ $a^2 \equiv -q^* [p']$, hence $\left(\frac{-q^*}{p'}\right) = 1$. Moreover,

$bp \equiv a^2 [q] \Rightarrow \left(\frac{bp}{q}\right) = 1$ and $bp \equiv q^* \equiv 1 [4]$; thus

$\left(\frac{b}{q}\right) = \left(\frac{p}{q}\right) \neq \left(\frac{-1}{p}\right) = \left(\frac{-1}{b}\right)$. It follows that there exists

$\underbrace{\qquad}_{(-1)^{\frac{b-1}{2}}}$.

a prime $p' \mid b$ $(\Rightarrow p' \neq 2, q)$ such that $\left(\frac{p'}{q}\right) \neq \left(\frac{-1}{p'}\right)$.

and $p' \leq b < p$

For such a prime (*) holds, by the above.

Case (II): $\boxed{q \mid a}$ $a = q^m A$, $m \geq 1$, $b = qB$, $q \nmid AB$,

$$q^{2m-1} A^2 = \underbrace{(-q^*/q)}_{-\left(\frac{-1}{q}\right)} + Bp.$$

Again, $(2ag\, B) = 1$ in this case, and $\forall$ prime $p' \mid B$ $a^2 \equiv -q^* \,[p']$, hence $\left(\frac{-q^*}{p'}\right) = 1$. Moreover, $Bp \equiv q^*/q \,[4q]$, which implies that $\left(\frac{Bp}{q}\right) = \left(\frac{q^*/q}{q}\right) = \left(\frac{-1}{q}\right)$ and $\left(\frac{-1}{Bp}\right) = q^*/q = \left(\frac{-1}{q}\right)$.

Therefore $\left(\frac{B}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) \neq \left(\frac{-1}{q}\right)\left(\frac{1}{p}\right) = \left(\frac{-1}{B}\right)$. It follows that there exists a prime $p' \mid B$ $(\Rightarrow p' \leq B < p)$ such that $\left(\frac{p'}{q}\right) \neq \left(\frac{-1}{p'}\right)$; for such a prime (*) holds.

Corollary. Fix q. If $QRL(p, q)$ holds for all

$$\left.\begin{cases} p \leq \frac{q+1}{2} & \text{if } q^* > 0 \\ p < q & \text{if } q^* < 0 \end{cases}\right\} \text{ satisfying } \left(\frac{p}{q}\right) \neq \left(\frac{-1}{p}\right),$$ then it

holds for all p satisfying $\left(\frac{p}{q}\right) \neq \left(\frac{-1}{p}\right)$.

Examples. (1) $q = 3$: $\left(\frac{p}{3}\right) \neq \left(\frac{-1}{p}\right) \Leftrightarrow p \equiv 5, 7 \,[12]$

So $QRL(p, 3)$: $\left(\frac{p}{3}\right) = \left(\frac{-3}{p}\right)$ holds if $p \equiv 5, 7 \,[12]$.

(2) $q = 5$: $\left(\frac{3}{5}\right) = -1 = \left(\frac{-1}{3}\right) \Rightarrow QRL(p, 5)$: $\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right)$ holds

if $\underbrace{\left(\frac{p}{5}\right) \neq \left(\frac{-1}{p}\right)}$

$p \equiv -1, -3, -7, -9 \,[20]$.

Combining descent for $x^2 \equiv \pm q^* [p]$:

Thm. Fix q. If $QRL(p,q)$ holds for all $p<q$ satisfying $\left(\frac{p}{q}\right)=-1$ or $\left(\frac{-1}{p}\right)=-1$, then it holds for all p satisfying ——— " ——— .

Examples: (1) $q=3$: $\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)$ holds if $\underbrace{p \not\equiv 1 [3] \text{ or } p \not\equiv 1 [4]}_{\iff p \not\equiv 1 [12].}$

(2) $q=5$: since $QRL(3,5)$ holds by (1),
$\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)$ holds if $\underbrace{p \not\equiv 1 [5] \text{ or } p \not\equiv 1 [4]}_{\iff p \not\equiv 1, 9 [20].}$

(3) $q=7$: since $QRL(3,7)$ and $QRL(5,7)$ hold,
$\left(\frac{-7}{p}\right)=\left(\frac{p}{7}\right)$ holds if $\underbrace{p \not\equiv 1,2,4 [7] \text{ or } p \not\equiv 1 [4]}_{\iff p \not\equiv 1, 9, 25 [28].}$

Pf of thm. If $\left(\frac{p}{q}\right)=-1$ (resp. if $\left(\frac{p}{q}\right)=1$ and $\left(\frac{-1}{p}\right)=-1$) the statement follows from Cor. of Descent for $x^2 \equiv q^* [p]$ (resp. for $x^2 \equiv -q^* [p]$).

Gauss' inductive proof of QRL

Historically, the first proof of QRL was given by Gauss, by an ingenious inductive procedure. We have already seen the first part of the proof (in a slightly different presentation): starting from the validity of QRL(3,5) and the formula $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, descent for $x^2 \equiv \pm q\,[p]$ can be used to prove inductively QRL(p,q) for $p > q$ such that $\left(\frac{p}{q}\right) = -1$ or $\left(\frac{-1}{p}\right) = -1$. Gauss' final step was to treat the remaining case $\left(\frac{p}{q}\right) = \left(\frac{-1}{p}\right) = 1$ $(p > q)$ by introducing an auxiliary odd prime $q' < p$ satisfying $\left(\frac{p}{q'}\right) = -1$ (and therefore satisfying QRL(p,q') by the first step), and then showing that QRL(p, qq') holds by performing descent for $x^2 \equiv qq'\,[p]$. ~~[illegible]~~. The statement of QRL(p,q) was then an immediate consequence.

The truly hard part was to show that $q' < p$ satisfying $\left(\frac{p}{q'}\right) = -1$ always exists (assuming that $\left(\frac{-1}{p}\right) = 1$). The descent for $x^2 \equiv qq'\,[p]$ was carried out by now very familiar arguments under the inductive (using) assumption that QRL(p_1, q_1) holds for all $p_1, q_1 < p$.

Earlier, descent for $x^2 \equiv \pm 2\,[p]$ was used to determine the values of $\left(\frac{2}{p}\right)$ for $p \not\equiv 1\,[8]$. Gauss then applied the same trick of introducing an auxiliary odd prime $q < p/2$ satisfying $\left(\frac{p}{q}\right) = -1$ to determine $\left(\frac{2}{p}\right)$ in the remaining case $p \equiv 1\,[8]$, by performing descent for $x^2 \equiv 2q\,[p]$ while relying on all previous results: QRL(p_1, q_1) for all p_1, q_1, and formulas for $\left(\frac{2}{p_1}\right)$ when $p_1 \not\equiv 1\,[8]$. That was a crowning achievement of a truly remarkable feat!

Descent for $x^2 \equiv q_1 q_2 [p]$

Descent lemma for $x^2 \equiv q_1 q_2 [p]$: Assume that:

(1) $p^* > 0$
(2) QRL(q, q') holds for all $q, q' < p$
(3) $q_1 \mid q_2 < p$
(4) $\left(\frac{p}{q_1 q_2}\right) = -1$

$\Rightarrow \left(\frac{q_1 q_2}{p}\right) = -1$ (in other words, QRL$(p, q_1 q_2)$ holds).

Cor. Assumptions (1)–(4) imply that both QRL(p, q_1) and QRL(p, q_2) hold.

Pf of Cor: $\exists i \in \{1,2\}$ $\left(\frac{p}{q_i}\right) = -1$. Descent lemma for $x^2 \equiv q_i^* [p]$ together with (2) imply that QRL(p, q_i) holds, and so does QRL$(p, q_1 q_2 / p_i)$.

Pf of Lemma. Assume that $\left(\frac{q_1 q_2}{p}\right) = 1$; we want to deduce a contradiction. There exist $a, b \in \mathbb{Z}$ such that

$a^2 = q_1 q_2 + bp, \quad 0 < a < p, \quad 2 \mid a \quad \Rightarrow \quad 2 \nmid b, \quad b \equiv -q_1 q_2 [4],$

$-p^2 < -q_1 q_2 < a^2 - q_1 q_2 = bp < a^2 < p^2 \quad \Rightarrow \quad |b| < p.$

Case (I,I): $\boxed{q_1 \nmid a, q_2 \nmid a}$ In this case $(2a q_1 q_2, bp) = 1$ and

$a^2 \equiv q_1 q_2 [|b|] \Rightarrow \left(\frac{q_1 q_2}{|b|}\right) = 1; \quad bp \equiv a^2 [q_i] \Rightarrow \left(\frac{bp}{q_i}\right) = 1 \Rightarrow \left(\frac{b}{q_1 q_2}\right) = \left(\frac{p}{q_1 q_2}\right) = -1$

Assumptions (2),(3) imply that $1 = \left(\frac{q_1 q_2}{|b|}\right) = \left(\frac{|b|^*}{q_1 q_2}\right) = \left(\frac{b^*}{q_1 q_2}\right)$, but

$b^*/b = -(q_1 q_2)^*/q_1 q_2$ and $\left(\frac{-m^*/m}{m}\right) = 1$ if $2 \nmid m$, $m > 0$;

therefore $\left(\frac{b^*/b}{q_1 q_2}\right) = 1$ and $1 = \left(\frac{b^*}{q_1 q_2}\right) = \left(\frac{b}{q_1 q_2}\right) = -1 \Rightarrow$ contradiction.

Case (II,II): $\boxed{q_1 \mid a, q_2 \nmid a}$ $a = q_1^m A, \ m \geq 1, \ b = q_1 B, \ q_i \nmid AB$

$q_1^{2m-1} A^2 = q_2 + Bp$. Again, $a^2 \equiv q_1 q_2 [|B|] \Rightarrow 1 = \left(\frac{q_1 q_2}{|B|}\right) \overset{(2)}{=} \left(\frac{|B|^*}{q_1 q_2}\right) = \left(\frac{B^*}{q_1 q_2}\right)$,

and $Bp \equiv -q_2 [q_1]$, $Bpq_1 \equiv a^2 [q_2]$, hence $\left(\frac{Bp}{q_1}\right) = \left(\frac{-q_2}{q_1}\right)$, $\left(\frac{Bp}{q_2}\right) = \left(\frac{q_1}{q_2}\right)$

and $\left(\frac{B}{q_1 q_2}\right) = \underbrace{\left(\frac{p}{q_1 q_2}\right)}_{-1}\left(\frac{-q_2}{q_1}\right)\left(\frac{q_1}{q_2}\right)$. However, $B \equiv -q_2 [4]$, $B^*/B = -q_2^*/q_2$,

hence $1 = \left(\frac{B^*}{q_1 q_2}\right) = \left(\frac{-q_2^*/q_2}{q_1}\right)\underbrace{\left(\frac{-q_2^*/q_2}{q_2}\right)}_{1}\left(\frac{B}{q_1 q_2}\right) = \underbrace{\left(\frac{-q_2^*/q_2}{q_1}\right)\left(\frac{-q_2}{q_1}\right)}_{\left(\frac{-q_2^*}{q_1}\right)}\left(\frac{q_1}{q_2}\right)(-1)$,

1, by (2),(3)

contradiction.

Case (I, II): $\boxed{q_1 \nmid a,\ q_2 \mid a}$ As in Case (II, I).

Case (II, II): $\boxed{q_1 \mid a,\ q_2 \mid a}$ $a = q_1^m q_2^n A$, $m, n \geq 1$, $b = q_1 q_2 B$, $q_i \nmid AB$

$$q_1^{2m-1} q_2^{2n-1} A^2 = 1 + Bp \implies 0 \equiv 1 + B \ [4] \implies |B|^* = B^* = -B$$

$$\Downarrow$$

$$Bp \equiv -1 \ [q_i] \implies \left(\frac{Bp}{q_i}\right) = \left(\frac{-1}{q_i}\right), \quad \left(\frac{-B}{q_1 q_2}\right) = \left(\frac{p}{q_1 q_2}\right)\left(\frac{\quad}{q_1 q_2}\right) = -1$$

As before, $a^2 \equiv q_1 q_2 \ [|B|]$, hence $1 = \left(\frac{q_1 q_2}{|B|}\right) \overset{(2)}{=} \left(\frac{|B|^*}{q_1 q_2}\right) = \left(\frac{-B}{q_1 q_2}\right) = -1$, contradiction.

Consequences of Descent for $x^2 \equiv \pm q^* \ [p]$ and $x^2 \equiv q_1 q_2 \ [p]$

Gauss observed that descent mechanism for $\nearrow$ and $\nwarrow$ can be used for an inductive proof of QRL, provided that one can establish the following (difficult) result (without using QRL, of course).

Key Auxiliary Thm (weak form). If $p \equiv 1 \ [4]$ is a prime, then there exists an odd prime $q < p$ such that $\left(\frac{p}{q}\right) = -1$.

Thm. QRL(p,q) holds for all p, q.

Pf (assuming Key Auxiliary Thm). For an integer $N \geq 1$, let $R(N)$ be the statement

$$\boxed{R(N): \quad \forall\, p, q < N \quad \text{QRL}(p,q) \text{ holds}}$$

$$\left(\Longrightarrow \quad \forall\ 1 < a, b < N \ \text{odd}, \ (a,b) = 1 \qquad \text{QRL}(a,b): \ \underbrace{\left(\frac{a}{b}\right) = \left(\frac{b^*}{a}\right)}_{\text{Jacobi symbol}} \text{ holds} \right)$$

$$b^* = \left(\frac{-1}{b}\right) b = (-1)^{(b-1)/2} b$$

$R(6)$ holds, since $\left(\frac{3}{5}\right) = -1 = \left(\frac{5}{3}\right)$.

Assume that $N \geq 6$ and $R(N)$ holds. We must show that $R(N+1)$ holds. This is automatic unless $N = P$ is a prime, which we assume. We must show that

QRL(P, q) holds for all $q < P$.

If $\left(\frac{P}{q}\right) = -1$ or $\left(\frac{-1}{P}\right) = -1$, then QRL$(P,q)$ is implied by (the validity of) QRL(p,q) for all $p < q$, by descent for $x^2 \equiv \pm q^* \ [p]$ (true by $R(P)$).

It remains to treat the case $\left(\frac{p}{q}\right) = 1 = \left(\frac{-1}{p}\right)$.
According to Key Auxiliary Thm, there exists $q' < p$ such that $\left(\frac{p}{q'}\right) = -1$ ($\Rightarrow q' \neq q$). Descent Lemma for $x^2 \equiv q_1 q_2 [p]$ then applies to $p = P$, $q_1 = q$ and $q_2 = q'$. Its Corollary tells us that QRL(P, q) holds, which concludes the proof of QRL (modulo validity of Key Auxiliary Thm).

Rmk 1. Note that, if one is allowed to use QRL, then the condition $\left(\frac{p}{q}\right) = -1$ in Key Auxiliary Thm is replaced by $\left(\frac{q}{p}\right) = -1$, which is trivially satisfied for some prime $q \neq 2$ if $p > 5$, since there are $\frac{p-1}{2}$ quadratic non-residues in the range $0 < x < p$ and they cannot all be of the form $\pm 2^a$, since $p \cdot \log_2(p) < \frac{p-1}{2}$ ($\Leftrightarrow p^2 < 2^{p-1}$) for $p > 7$ (and $\left(\frac{-1}{p}\right) = -1$).

Rmk 2. One can treat the two descent arguments for $x^2 \equiv \pm q^* [p]$ simultaneously, by considering $x^2 \equiv \varepsilon q^* [p]$, $\varepsilon = \pm 1$. As QRL(p, q) is equivalent to $\left(\frac{\varepsilon q^*}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{p}{q}\right)$, the statements become as follows.

Descent Lemma for $x^2 \equiv \varepsilon q^* [p]$: Fix $\varepsilon = \pm 1$ and q. If

(*) $\left(\frac{p}{q}\right) = -\left(\frac{\varepsilon}{p}\right)$ and $\left(\frac{\varepsilon q^*}{p}\right) = 1$

and $p > \begin{cases} q & \text{if } \varepsilon q^* > 0 \\ (q+1)/2 & \text{if } \varepsilon q^* < 0 \end{cases}$, then $\exists\, p' < p$ satisfying (*).

Cor. Fix $\varepsilon = \pm 1$ and q. If QRL(p, q) holds for all $p < q$ satisfying $\left(\frac{p}{q}\right) = -\left(\frac{\varepsilon}{p}\right)$, it holds for all p satisfying $\left(\frac{p}{q}\right) = -\left(\frac{\varepsilon}{p}\right)$.

Thm (= Cor. of Cor.) (Fix q.) If QRL(p, q) holds for all $p < q$ satisfying $\left(\frac{p}{q}\right) = -1$ or $\left(\frac{-1}{p}\right) = -1$, it holds for all p satisfying

Existence of small q such that $\left(\frac{p}{q}\right)=-1$ $(p\equiv 1[4])$

Warm-up: **Prop.** $p\equiv 1[4]$ prime $\Rightarrow \exists$ odd prime $q<p$, $\left(\frac{-p}{q}\right)=-1$.

$p\neq 5$

Pf. Let $a-1<\sqrt{p}/2<a$ $(a\in\mathbb{Z})$. Then $0<4a^2-p<p$ if $p\neq 17, 5$

$4a^2-p\equiv -1[4] \Rightarrow \exists$ prime $q\mid(4a^2-p)$, $q\equiv -1[4]$

As $(2a)^2\equiv p\,[q]$, $\left(\frac{p}{q}\right)=1$ and $\left(\frac{-p}{q}\right)=\left(\frac{-1}{q}\right)=-1$.

Easy case: $p\equiv 5[8]$ prime $\Rightarrow \exists$ odd prime $q<p$, $\left(\frac{p}{q}\right)=-1$

(in fact, $q<\sqrt{8p}$)

Pf: If $0<a<\sqrt{p/2}$, $a\in\mathbb{Z}$, then $0<p-2a^2\equiv\pm 5[8]$

$\Rightarrow \exists$ prime $q\mid(p-2a^2)$, $q\equiv\pm 5[8]$. Then $q<p$ and

$p\equiv 2a^2[q] \Rightarrow \left(\frac{p}{q}\right)=\left(\frac{2}{q}\right)=-1$. If we take $a=[\sqrt{p/2}]$, then

$2a^2>2(\sqrt{p/2}-1)^2=p-2\sqrt{2p}+2 \Rightarrow q<2\sqrt{2p}-2<\sqrt{8p}$.

Difficult case: $p\equiv 1[8]$ prime $\Rightarrow \exists$ odd prime $q<\sqrt{p}$, $\left(\frac{p}{q}\right)=-1$

(Gauss proved this with $q<2\sqrt{p}$; the bound $q<\sqrt{p}$ is Tate's (?) improvement).

Pf. Let $0<N=\prod_{\substack{2+k\\ k^2<p}} \frac{p-k^2}{4}=\frac{(\sqrt{p}+1)(\sqrt{p}-1)}{4}\cdot\frac{(\sqrt{p}+3)(\sqrt{p}-3)}{4}\cdots\frac{(\sqrt{p}+m)(\sqrt{p}-m)}{4}$

$(2+m<\sqrt{p}<m+2)$

$$<\prod_{\substack{k=1\\ 2+k}}^{m}\frac{m+2+k}{2}\cdot\frac{m+2-k}{2}=(m+1)!$$

contradiction

Claim: If $\left(\frac{p}{q}\right)=1$ for all odd primes $q<\sqrt{p}$, then $(m+1)!\mid N$

Pf of claim: $\Rightarrow \forall r\geq 1$ $\exists\, x_{q^r}\in\mathbb{Z}$ $x_{q^r}^2\equiv p\,[4q^r]$.

$p\equiv 1[8] \Rightarrow \forall r\geq 1$ $\exists\, x_{2^r}\in\mathbb{Z}$ $x_{2^r}^2\equiv p\,[4\cdot 2^r]$.

As $(m+1)!=\prod_{\ell^r\leq m+1}\ell^{[(m+1)/\ell^r]}$ (ℓ prime, $r\geq 1$), we need to show that whenever $\ell^r\leq m+1$, there are at least $\left[\frac{m+1}{\ell^r}\right]$ among the factors $\frac{p-k^2}{4}$ of N that are divisible by ℓ^r. (Note: if $\ell^r\leq m+1$, $\ell\neq 2\Rightarrow \ell\leq m<\sqrt{p}$).

We know that $\exists\, x=x_{\ell^r}\in\mathbb{Z}$ such that $x^2\equiv p\,[4\ell^r]$. Given such x, $\pm x+2\ell^r n$ $(n\in\mathbb{Z})$ is also a solution, so we can assume that $0<x<\ell^r$, which produces solutions, $\ell^r<2\ell^r-x<2\ell^r$, $2\ell^r<x+2\ell^r<3\ell^r$, etc., hence at least $\left[\frac{m+1}{\ell^r}\right]$ solutions among $\{1,\dots,m+1\}$, as claimed.

$\left(\frac{2}{p}\right)=1$ for $p\equiv 1\,[8]$ via descent for $x^2\equiv 2q\,[p]$

Descent lemma for $x^2\equiv 2q\,[p]$:

Assume that: (1) $p\equiv 1\,[8]$

(2) $\left(\frac{2}{p}\right)=-1$

(3) $q<p/2$

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

(5) QRL(p_1,q_1) holds for all p_1,q_1

(6) $\left(\frac{2}{p_1}\right)=-1$ if $p_1\not\equiv\pm 1\,[8]$, and $\left(\frac{-2}{p_2}\right)=-1$ if $p_2\not\equiv 1,3\,[8]$

$\exists\, p'<p$, $p\equiv 1\,[8]$, $\left(\frac{2}{p'}\right)=-1$.

Cor. $\forall\, p\equiv 1\,[8]$ $\left(\frac{2}{p}\right)=1$ (assuming the validity of (5), (6) above).

Pf of Cor: Assumption (5) implies immediately that an odd prime $q<p/2$ satisfying $-1=\left(\frac{p}{q}\right)$ $\left(=\left(\frac{q}{p}\right)\right)$ exists for each prime $p\equiv 1\,[8]$:

there are $\frac{p-1}{4}$ quadratic non-residues (mod p) in the range $0<x<p/2$, and they cannot all be of the form $\pm 2^a$, since $\left(\frac{-1}{p}\right)=1$ and $\log_2((p-1)/2)<(p-1)/4$ for $(p>1)/2>2$. Descent lemma then implies that the assumption $p\equiv 1\,[8]$, $\left(\frac{2}{p}\right)=-1$ leads to a contradiction, by infinite descent.

Pf of Descent Lemma: it follows from (4), (5) that $\left(\frac{q}{p}\right)=-1$; thus $\left(\frac{2q}{p}\right)=1$. There exist $a,b\in\mathbb{Z}$ such that

$a^2=2q+bp$, $0<a<p$, $2\nmid a$ $\Rightarrow$ $b\equiv -1\,[4]$, $1-p\le 1-2q\le bp<a^2<p^2\Rightarrow 0<b<p$

In fact, $1\equiv a^2\equiv 2q+b\,[8]$, hence $-b\equiv\begin{cases}1\,[8], & q^*>0\\ 5\,[8], & q^*<0\end{cases}$.

Case (I): $\boxed{2\nmid a}$ $(2aq,bp)=1$. Let us write $b=b_1b_{-1}b_5b_{-5}$, where each b_k is a product of n_k primes (not necessarily distinct) $p_k\equiv k\,[8]$ $(k=\pm 1,\pm 5)$. Let us compute $\left(\frac{-1}{b}\right)$ and $\left(\frac{2}{b}\right)$, and similarly for each b_k; after that we compare the results.

$\left(\frac{-1}{b_k}\right) = \begin{cases} 1, & k=1,5 \\ (-1)^{n_k}, & k=-1,-5 \end{cases}$; $\left(\frac{2}{b_k}\right) = \begin{cases} 1, & k=\pm 1 \\ (-1)^{n_k}, & k=\pm 5 \end{cases}$ (by (6))

$\left(\frac{-1}{b}\right) = -1$, [illegible]. As a result,

$-1 = (-1)^{n_{-1}+n_{-5}}$, $\left(\frac{2}{b}\right) = (-1)^{n_5+n_{-5}}\left(\frac{2}{b_1}\right)$

On the other hand, $a^2 \equiv 2q\ [b]$, hence $\left(\frac{2q}{b}\right) = 1$ (Jacobi symbol again)

and $\left(\frac{2}{b}\right) = \left(\frac{q}{b}\right) \overset{(5)}{=} \left(\frac{b^*}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{b}{q}\right)$. Similarly, $a^2 \equiv bp\ [q]$, hence

[illegible] $\left(\frac{bp}{q}\right) = 1$ and $\left(\frac{b}{q}\right) = \left(\frac{p}{q}\right) = -1$. therefore

$\left(\frac{2}{b}\right) = -\left(\frac{-1}{q}\right)$. Finally, [illegible]

$-b = (-1)^{n_{-1}+n_{-5}} b \equiv 5^{n_5+n_{-5}}\ [8] \Rightarrow n_5+n_{-5} \equiv \begin{cases} 0\ [2], & q^*>0 \\ 1\ [2], & q^*<0, \end{cases}$

hence $(-1)^{n_5+n_{-5}} = \left(\frac{-1}{q}\right)$. Putting everything together, we obtain

$\left(\frac{2}{b_1}\right) = (-1)^{n_5+n_{-5}}\left(\frac{2}{b}\right) = \underbrace{(-1)^{n_5+n_{-5}}\left(\frac{-1}{q}\right)}_{1}\underbrace{\left(\frac{2}{b}\right)\left(\frac{p}{q}\right)}_{-1} = -1$. therefore

$\exists$ prime $p' \mid b_1$ ($\Rightarrow p' \equiv 1\ [8]$, $p' \le b < p$) satisfying $\left(\frac{2}{p'}\right) = -1$, as claimed.

Case (II): $\boxed{q \mid a}$ $a = q^m A$, $m \ge 1$, $b = qB$, $q \nmid AB$

$q^{2m-1}A^2 = 2 + Bp$; write [illegible] $B = b_1 b_{-1} b_5 b_{-5}$ as before.

We have again $a^2 \equiv 2q\ [B] \Rightarrow \left(\frac{2}{B}\right) = \left(\frac{q}{B}\right) \overset{(5)}{=} \left(\frac{B^*}{q}\right) = \left(\frac{-2^*/q}{q}\right)\left(\frac{B}{q}\right)$

$-1 = b^*/b = (B^*/B)(2^*/2)$ ($\underbrace{\ }_{1}$)

$Bp \equiv -2\ [q] \Rightarrow \left(\frac{B}{q}\right) = \left(\frac{-2p}{q}\right) = \left(\frac{-2}{q}\right)\overbrace{\left(\frac{p}{q}\right)}^{-1}$, hence [illegible]

$-q \equiv B \equiv (-1)^{n_{-1}+n_{-5}}\ [4] \Rightarrow (-1)^{n_{-1}+n_{-5}} = -\left(\frac{-1}{q}\right)$

[illegible] As before, $\left(\frac{2}{B}\right) = \left(\frac{2}{B_1}\right)(-1)^{n_5+n_{-5}}$ and

$5^{n_5+n_{-5}} \equiv \underbrace{(-1)^{n_{-1}+n_{-5}}}_{-\left(\frac{-1}{q}\right)} \underbrace{B}_{\equiv q-2\ [8]}\ [8] \Rightarrow (-1)^{n_5+n_{-5}} = \begin{cases} 1, & q \equiv 1,3\ [8] \\ -1, & q \equiv 5,7\ [8] \end{cases}$

Therefore: $\left(\frac{2}{B_1}\right) = \left(\frac{2}{B}\right)(-1)^{n_5+n_{-5}}$, $\left(\frac{2}{B}\right) = \left(\frac{B}{q}\right) = \left(\frac{-2}{q}\right)\left(\frac{p}{q}\right) = -\left(\frac{-2}{q}\right)$

$$-\left(\frac{2}{B_1}\right) = \left(\frac{-2}{q}\right)(-1)^{n_5+n_{-5}} = \left(\frac{2}{q}\right)\cdot\begin{cases} 1, & q\equiv\pm1\,[8] \\ -1, & q\equiv\pm5\,[8] \end{cases} \overset{(6)}{=} \begin{cases} \left(\frac{2}{q}\right), & q\equiv 1\,[8] \\ 1, & q\not\equiv 1\,[8], \end{cases}$$

hence $\left(\frac{2}{B_1}\right) = \left(\frac{2}{B_1}\right)\cdot\begin{cases} \left(\frac{2}{q}\right), & q\equiv 1\,[8] \\ 1, & q\not\equiv 1\,[8] \end{cases} = -1$. As a result,

$\exists\ p' \mid b_1$ such that $\left(\frac{2}{p'}\right) = -1$, as claimed.

$(\Rightarrow\ p'\equiv 1\,[8],\ p' \le b_1 \le b < p)$

Rmk. the question of giving an upper bound on the smallest $a>1$ such that $\left(\frac{a}{p}\right) = -1$ (a is necessarily a prime) has been treated extensively by analytic methods.

It is expected that $a < C(\varepsilon)\,p^{\varepsilon}$, for any $\varepsilon > 0$ (regardless of the value of $p \pmod 4$).

The argument of Gauss gives bounds $a < \sqrt{8p}$ if $p\equiv 5\,[8]$ and $a < 2\sqrt{p}$ (improved to $a<\sqrt{p}$ by Tate) if $p\equiv 1\,[8]$.

the Pólya–Vinogradov Thm implies that $a < \sqrt{p}\,\ln(p)$.

$\forall x \ge 1 \quad \sum_{n\le x}\left(\frac{n}{p}\right) < \sqrt{p}\,\ln(p)$

easy consequence of discrete Fourier transform

Much more involved analytic arguments were necessary to obtain bounds (Vinogradov, Burgess, ...
