Quadratic Residues Part II

Let p be prime

Recall that n is a quadratic residue $\bmod p \iff n \equiv k^2 \bmod p$ for some k coprime to p.

The Legendre symbol $\left(\frac{n}{p}\right)$ is defined if p is prime and n coprime to p:

$\left(\frac{n}{p}\right) = 1$ if n is a quadratic residue $\bmod p$

$= -1$ otherwise.

Examples $\left(\frac{3}{5}\right) = -1$ because $1 \equiv 1^2 \equiv 4^2$ and $4 \equiv 2^2 \equiv 3^2$ are the quadratic residues $\bmod 5$

$\left(\frac{2}{7}\right) = 1$ because $2 \equiv 3^2 \bmod 7$

$\left(\frac{-1}{5}\right) = 1$ because $-1 \equiv 4 \equiv 2^2 \bmod 5$

In fact we have already seen that $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \bmod 4$.

$\left(\frac{1}{p}\right) = 1$ for all primes p, because $1 = 1^2$.

Theorem Let p be an odd prime and n coprime to p. Then

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \bmod p.$$

Proof. Note that for all n coprime to p, $n^{p-1} \equiv 1 \bmod p$, by Fermat's Little Theorem. Hence, if $x = n^{\frac{p-1}{2}}$, $x^2 \equiv 1 \bmod p$ and $(x-1)(x+1) \equiv 0 \bmod p$. Hence $x \equiv \pm 1 \bmod p$, that is $n^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$

Let a be a primitive element mod p.

Then a^m is a quadratic residue $\Leftrightarrow$ $a^m = (a^k)^2$ for some $0 < k < p-1$ $\Rightarrow$ $(a^m)^{\frac{p-1}{2}} \equiv (a^k)^{p-1} \equiv (a^{p-1})^k \equiv 1 \bmod p$

Conversely, if $a^{m(\frac{p-1}{2})} \equiv 1$ then since a is primitive — of order $p-1$, — $p-1 \mid m(\frac{p-1}{2})$ that is, $\frac{m}{2}$ must be an integer and m is even.

So if n is coprime to p then $n \equiv a^m$ for some m

and hence $n^{\frac{p-1}{2}} \equiv 1 \Leftrightarrow n$ is a quadratic residue mod p

that is $n^{\frac{p-1}{2}} = 1 \Leftrightarrow \left(\frac{n}{p}\right) = 1$

Hence (since $n^{\frac{p-1}{2}} = \pm 1$) $n^{\frac{p-1}{2}} = \left(\frac{n}{p}\right)$

Corollary If n_1 and n_2 are coprime to a prime p,

$$\left(\frac{n_1 n_2}{p}\right) = \left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right)$$

Proof $\left(\frac{n_1 n_2}{p}\right) \equiv (n_1 n_2)^{\frac{p-1}{2}} \equiv n_1^{\frac{p-1}{2}} n_2^{\frac{p-1}{2}} \equiv \left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right) \bmod p$

If p is an odd prime since both sides are ± 1 we have

$$\left(\frac{n_1 n_2}{p}\right) = \left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right)$$

If $p = 2$ it is still true because $\left(\frac{n_1}{p}\right) = \left(\frac{n_2}{p}\right) = \left(\frac{n_1 n_2}{p}\right) = 1$

Theorem Let p be any odd prime. Then

$$\left(\frac{2}{p}\right) = 1 \text{ if } p = \pm 1 \bmod 8$$
$$= -1 \text{ if } p = \pm 3 \bmod 8$$

Examples If $p = 3$ or 5 then 2 is not a quadratic residue mod p

If $p = 7$ then $2 \equiv 3^2 \bmod 7$

If $p = 17$ then $2 \equiv 6^2 \bmod 17$.

Proof of Theorem Let p be any odd prime

If k is coprime to p then there is a unique integer $(k)_p$ such that $(k)_p \equiv k \bmod p$

$$-\left(\frac{p-1}{2}\right) \leq (k)_p \leq \frac{p-1}{2}$$

$(k)_p$ can take any integer value in this range apart from 0.

Note $(-k)_p = -(k)_p$

Now consider the integers $(2i)_p$ for $1 \leq i \leq \frac{p-1}{2}$ $1,2,3,4,5,6,7,8$
$\to 2,4,6,8,10,12,14,16$
$\to 2,4,6,8,-7,-5,-3,-1$

Claim if $1 \leq i < j \leq \frac{p-1}{2}$ then $(2i)_p \neq \pm (2j)_p$. $1,2,3 \to 2,4,6$

$p=17$ $\to 2,5,-1$

If $(2i)_p = (2j)_p$ then $2i \equiv 2j \bmod p$ and $i \equiv j \bmod p$ $\dot{\times}$ $m=8$

If $(2i)_p = -(2j)_p$ then $(2i)_p = (-2j)_p$ and $2i \equiv -2j \bmod p$

and $i \equiv -j \bmod p$ This is impossible because $-j \geq -\left(\frac{p-1}{2}\right)$

and hence $0 < |i+j| < p$ (for $0 < i+j \leq p-2$) $\dot{\times}$.

Let $m = \#\{i : (2i)_p < 0\}$

(88)

Then $(2.1)_p \cdots (2.(\frac{p-1}{2}))_p = (-1)^m (1 \cdots (\frac{p-1}{2}))$

But $(2.1)_p \cdots (2(\frac{p-1}{2}))_p \equiv 2^{\frac{p-1}{2}} \cdot (1 \cdots \frac{p-1}{2}) \mod p.$

So $(-1)^m (\underbrace{1 \cdots \frac{p-1}{2}}_{\text{coprime to } p}) \equiv 2^{\frac{p-1}{2}} (1 \cdots (\frac{p-1}{2})) \mod p$

So $(-1)^m \equiv 2^{\frac{p-1}{2}} \mod p.$

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

So to prove the theorem it remains to show that

m is even $\iff p \equiv \pm 1 \mod 8.$

Case $p \equiv 1 \mod 8$ $\quad p = 8k+1$, some $k \in \mathbb{Z}_+$

$\frac{p-1}{2} = 4k.$ If $1 \le i \le 2k$ then $2.1 \le \underbrace{2.i}_{(2i)_p} \le 4k = \frac{p-1}{2}$

If $\underbrace{2k+1 \le i \le 4k}_{2k \text{ such } i}$ then $\underbrace{1-4k}_{-(\frac{p-1}{2})} \le \underbrace{2i-8k-1}_{(2i)_p} \le 8k-8k-1 = -1$

$-4k = -(\frac{p-1}{2}) < 1-4k$

So $m = 2k$ is even as required

Case $p \equiv -1 \mod 8$ $\quad p = 8k-1$, some $k \in \mathbb{Z}_+$

$\frac{p-1}{2} = 4k-1 = \frac{8k-2}{2}$ If $1 \le i \le 2k-1$ then $2 \le \underbrace{2.i}_{(2i)_p} \le 4k-2 = \frac{p-1}{2}$

If $\underbrace{2k \le i \le 4k-1}_{2k \text{ such } i}$ then $2.2k-(8k-1) = 1-4k = -(\frac{p-1}{2})$

$-(\frac{p-1}{2}) = 2.2k-(8k-1) \le \underbrace{2.i-(8k-1)}_{(2.i)_p} \le 8k-2-(8k-1) = -1$

So $m = 2k$ is even as required

(99)

$p \equiv 3 \bmod 8$ $\quad p = 8k+3$, some $k \in \mathbb{N}$

$\frac{p-1}{2} = \frac{8k+2}{2} = 4k+1$

$1 \le i \le 2k \implies 2 \le (2.i)_p \le 4k < \frac{p-1}{2}$

$\underbrace{2k+1 \le i \le 4k+1}_{2k+1 \text{ choices}} \implies 2.(2k+1) - (8k+3) = \underbrace{-(4k+1)}_{-\left(\frac{p-1}{2}\right)} \le \underbrace{2i-(8k+3)}_{(2i)_p} \le 2(4k+1) - (8k+3) = -1$

So $m = 2k+1$ is odd as required

$p \equiv -3 \bmod 8$ $\quad p = 8k-3$, some $k \in \mathbb{Z}_+$

$\frac{p-1}{2} = \frac{8k-4}{2} = 4k-2$

$1 \le i \le 2k-1 \implies 2 \le \underbrace{2i}_{(2.i)_p} \le 4k-2 < \frac{p-1}{2}$

$\underbrace{2k \le i \le 4k-2}_{2k-1 \text{ choices}} \implies \overset{-\left(\frac{p-1}{2}\right) <}{\wedge} 4k-(8k-3) = 3-4k \le \underbrace{2i-(8k-3)}_{(2i)_p}$

$\le 8k-4-(8k-3) = -1$

So $m = 2k-1$ is odd as required

Theorem -2 is a quadratic residue mod $p \iff$

$p \equiv 1$ or $3 \bmod 8$

Proof $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1 \iff \begin{cases} \left(\frac{-1}{p}\right) = 1 \text{ and } \left(\frac{2}{p}\right) = 1 \\ \text{or } \left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1 \end{cases}$

$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \bmod 4 \iff p \equiv 1 \bmod 8$ or $p \equiv 5 \equiv -3 \bmod 8$

So $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1 \iff p \equiv 1 \bmod 8$

and $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1 \iff p \equiv 3 \bmod 8.$

Quadratic reciprocity

Theorem Let p and q be ~~odd~~ distinct odd primes, $p \neq \pm q$

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

Equivalently, $\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}\left(\frac{p}{q}\right)$

(Just multiply both sides of the first equation by $\left(\frac{p}{q}\right)$, which is ± 1)

Remark if either $\frac{p-1}{2}$ or $\frac{q-1}{2}$ is even then

$\frac{(p-1)(q-1)}{4} = \frac{p-1}{2} \times \frac{q-1}{2}$ is even and $\left(\frac{p}{q}\right) = +\left(\frac{q}{p}\right)$

So in these cases p is a quadratic residue mod q

$\Leftrightarrow$ q is a quadratic residue mod p.

Remark The result holds for any ~~distinct~~ odd primes p and q, positive or negative, provided $p \neq \pm q$

Examples

(1) Compute $\left(\frac{11}{13}\right)$

$\left(\frac{11}{13}\right)\left(\frac{13}{11}\right) = (-1)^{6\times 5} = 1$

So $\left(\frac{11}{13}\right) = \left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = -1$ because $11 \equiv 3 \bmod 8$

(2) $\left(\frac{43}{103}\right)\left(\frac{103}{43}\right) = (-1)^{51\times 21} = -1$

$\left(\frac{43}{103}\right) = -\left(\frac{103}{43}\right) = -\left(\frac{103-86}{43}\right) = -\left(\frac{17}{43}\right)$

$\left(\frac{17}{43}\right)\left(\frac{43}{17}\right) = (-1)^{8\times 21} = 1$ $\quad -\left(\frac{17}{43}\right) = -\left(\frac{43}{17}\right) = -\left(\frac{9}{17}\right) = -1$

because $9 = 3^2$

(3) $\left(\frac{30}{1019}\right) = \left(\frac{2 \cdot 3 \cdot 5}{1019}\right) = \left(\frac{2}{1019}\right)\left(\frac{3}{1019}\right)\left(\frac{5}{1019}\right)$

$1019 \equiv 3 \bmod 8$ so $\left(\frac{2}{1019}\right) = -1$

$\left(\frac{3}{1019}\right) \cdot \left(\frac{1019}{3}\right) = (-1)^{1 \times 509} = -1$

$\left(\frac{1019}{3}\right) = \left(\frac{2}{3}\right) = -1$ So $\left(\frac{3}{1019}\right) = 1$

$\left(\frac{5}{1019}\right)\left(\frac{1019}{5}\right) = (-1)^{4 \times 509} = 1$

So $\left(\frac{5}{1019}\right) = \left(\frac{1019}{5}\right) = \left(\frac{4}{5}\right) = 1$ because $4 = 2^2$

So $\left(\frac{30}{1019}\right) = -1 \times 1 \times 1 = -1$

(4) $\left(\frac{31}{1019}\right)\left(\frac{1019}{31}\right) = (-1)^{15 \times 509} = -1$

$992 = 31 \times 32$

$\left(\frac{1019}{31}\right) = \left(\frac{27}{31}\right) = \left(\frac{-4}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{4}{31}\right) = -1 \times 1$ because $31 \equiv -1 \bmod 4$

So $\left(\frac{31}{1019}\right) = +1$

(5) $\left(\frac{29}{1019}\right)\left(\frac{1019}{29}\right) = (-1)^{28 \times 509} = 1$

$1015 = 35 \times 29$

So $\left(\frac{29}{1019}\right) = \left(\frac{1019}{29}\right) = \left(\frac{4}{29}\right) = 1$

Another method for (4) From $\left(\frac{1019}{31}\right) = \left(\frac{27}{31}\right) = \left(\frac{3}{31}\right)^3$

We have $\left(\frac{3}{31}\right)\left(\frac{31}{3}\right) = (-1)^{15 \times 1} = -1$

So $\left(\frac{3}{31}\right) = -\left(\frac{31}{3}\right) = -\left(\frac{1}{3}\right) = -1$. So $\left(\frac{1019}{31}\right) = -1$ again

and $\left(\frac{31}{1019}\right) = 1$

Proof of Quadratic reciprocity

First do it when p and q are positive distinct primes.

As in the case of $q = 2$ first show that $\left(\frac{q}{p}\right) = (-1)^m$ where m is defined as follows.

For i coprime to p define i_p to be the integer such that

$i_p \equiv i \bmod p$

$$-\left(\frac{p-1}{2}\right) \leq i_p \leq \frac{p-1}{2}.$$

Note $i_p \neq 0$ Also $(-i)_p = -(i_p)$

Let $m = \#\left\{ i : (qi)_p < 0, \quad 1 \leq i \leq \frac{p-1}{2} \right\}$

As before if $1 \leq i < j \leq \frac{p-1}{2}$

$(qi)_p \neq \pm (qj)_p$

If $(qi)_p = (qj)_p$ then $qi \equiv qj \bmod p \Rightarrow i \equiv j \bmod p$ ✗.

If $(qi)_p = -(qj)_p$ then $(qi)_p = (-qj)_p$ as

$qi \equiv -qj \bmod p \Rightarrow i \equiv -j \bmod p$

But $2 \leq i+j \leq \frac{p-3}{2} + \frac{p-1}{2}$ $\quad 0 < i-(-j) < p$

So $i \not\equiv -j \bmod p$ ✗

So $(q \cdot 1)_p \cdots (q \cdot \frac{p-1}{2}) \equiv (-1)^m \left(1 \cdots \frac{p-1}{2}\right) \bmod p$

$$q^{\frac{p-1}{2}} \cdot \underbrace{\left(1 \cdots \frac{p-1}{2}\right)}_{\text{coprime to } p} \equiv (-1)^m \left(1 \cdots \frac{p-1}{2}\right) \bmod p$$

So $q^{\frac{p-1}{2}} = (-1)^m \bmod p.$

So $\left(\frac{q}{p}\right) = (-1)^m$

Now we want to reinterpret this

Lemma $m \equiv M \bmod 2$ where

$$M = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \quad \text{where } \lfloor x \rfloor = \text{largest integer} \le x$$

Hence $(-1)^m = (-1)^M$

Proof. $\left\lfloor \frac{iq}{p} \right\rfloor = \frac{iq}{p} - \frac{1}{p}(iq)_p$ if $(iq)_p > 0$

$= \frac{iq}{p} - \frac{1}{p}(iq)_p - 1$ if $(iq)_p < 0$

$$p\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor = q\sum_{i=1}^{\frac{p-1}{2}} i - \sum_{i=1}^{\frac{p-1}{2}} (iq)_p - mp$$

$(x)_p \equiv |(x)_p| \bmod 2$ for any integer x

For $1 \le i \le \frac{p-1}{2}$, $|(iq)_p|$ takes each value $1 \le j \le \frac{p-1}{2}$ exactly once

p, q odd. $p \equiv 1 \bmod 2$ $q \equiv 1 \bmod 2$

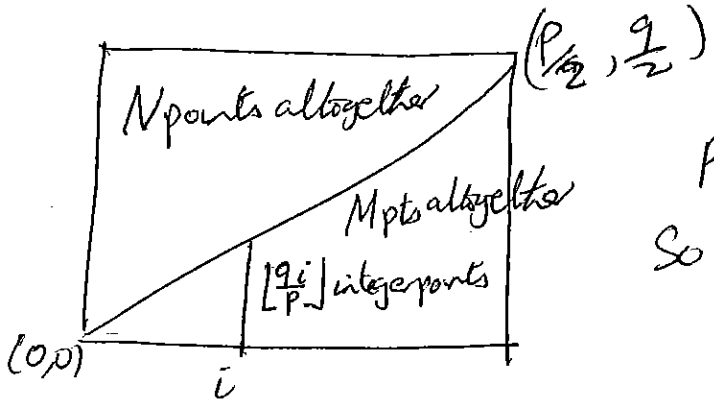
So $\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \equiv p\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \equiv q\sum_{i=1}^{\frac{p-1}{2}} i - \sum_{j=1}^{\frac{p-1}{2}} |(iq)_p| - m \bmod 2$

$$\equiv \sum_{i=1}^{\frac{p-1}{2}} i - \sum_{j=1}^{\frac{p-1}{2}} j + m \equiv m \bmod 2.$$

Lemma $M = \#\{(i,j) \in \mathbb{Z}^2 : 1 \le i \le \frac{p-1}{2},\ 1 \le j \le \frac{q-1}{2} \text{ \&, } pj \le qi\}$

Proof For any integer j, $pj \le qi \iff j \le \left\lfloor \frac{qi}{p} \right\rfloor$

Proof of Quadratic reciprocity



p, q coprime $\Rightarrow pj = qi$ not possible

So no points on line $y = \frac{q}{p}x$

$$M + N = \frac{p-1}{2} \times \frac{q-1}{2} = \frac{(p-1)(q-1)}{4}$$

$$\text{So } \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Quadratic reciprocity for negative integers

To deduce quadratic reciprocity for $(p, -q)$ from quad. rec for (p, q):

$$\frac{-q-1}{2} + \frac{q-1}{2} \equiv \frac{q-1}{2} + 1 \mod 2$$

$$\text{So } (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{-q-1}{2}\right)} = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} \iff \frac{p-1}{2} \text{ is even}$$

$$\iff p \equiv 1 \mod 4 \iff \left(\frac{-1}{p}\right) = 1$$

$$\left(\frac{p}{q}\right) = \left(\frac{p}{-q}\right) \text{ because } p \equiv x^2 \mod q \iff p \equiv x^2 \mod (-q)$$

(p, q coprime)

$$\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right) \iff p \equiv 1 \mod 4.$$

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

Examples

① $\left(\frac{-3}{p}\right)\left(\frac{p}{-3}\right) = (-1)^{-2\times\frac{(p-1)}{2}} = 1$ $\forall$ odd primes $|p| > 3$

So $\left(\frac{-3}{p}\right) = \left(\frac{p}{-3}\right) = \left(\frac{p}{3}\right)$ $\forall$ odd primes $|p| > 3$

$\left(\frac{p}{3}\right) = 1$ if $p \equiv 1 \bmod 3$ $p > 3$

$= -1$ if $p \equiv 2 \bmod 3$ $p > 3$

So -3 is a quadratic residue mod $p \iff p \equiv 1 \bmod 3$

$\forall$ odd primes $p > 3$

② When is 3 a quadratic residue mod p, for p a prime > 3?

$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{1\times\frac{(p-1)}{2}}$ $= 1$ if $p \equiv 1 \bmod 4$

$= -1$ if $p \equiv 3 \bmod 4$

$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ if $p \equiv 1 \bmod 4$

$= -\left(\frac{p}{3}\right)$ if $p \equiv 3 \bmod 4$

So $\left(\frac{3}{p}\right) = 1$ if $p \equiv 1 \bmod 4$ and $p \equiv 1 \bmod 3$, that is, $p \equiv 1 \bmod 12$

or if $p \equiv 3 \equiv -1 \bmod 4$ and $p \equiv -1 \bmod 3$, that is $p \equiv -1 \bmod 12$

If p is prime, $p > 3$ then $p \equiv 1, 5, 7, 11 \bmod 12$, that is,

$p \equiv \pm 1$ or $\pm 5 \bmod 12$.

$\left(\frac{3}{p}\right) = 1$ if $p \equiv \pm 1 \bmod 12$

-1 if $p \equiv \pm 5 \bmod 12$

Applications to sums of squares.

We now know $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \bmod 8$

$\left(\frac{-2}{p}\right) = 1 \iff p \equiv 1 \text{ or } 3 \bmod 8$

$\left(\frac{3}{p}\right) = 1 \iff p \equiv \pm 1 \bmod 12$

$\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \bmod 3$

Theorem $n \in \mathbb{Z} \setminus \{0\}$ can be written as $a^2 - 2b^2$ for $a, b \in \mathbb{Z} \iff n = \pm N^2 2^k \prod_{i=1}^{l} p_i$ for $N \in \mathbb{Z}_+$, $k \geq 0$, $l \geq 0$ integers and p_i are positive primes which are all $\pm 1 \bmod 8$ $\left(\left(\frac{2}{p_i}\right) = 1\right)$

Theorem $n \in \mathbb{Z}_+$ can be written as $a^2 + 2b^2$ for $a, b \in \mathbb{Z} \iff$ $n = N^2 2^k \prod_{i=1}^{l} p_i$ for $N \in \mathbb{Z}_+$, integers $k, l \geq 0$ and p_i are positive primes which are all 1 or 3 mod 8 $\left(\left(\frac{-2}{p_i}\right) = 1\right)$

Theorem $n \in \mathbb{Z}_+$ can be written as $a^2 + 3b^2$ for $a, b \in \mathbb{Z}$ $\iff n = N^2 3^k \prod_{i=1}^{l} p_i$ for $N \in \mathbb{Z}_+$, $k, l \in \mathbb{N}$, p_i are all positive primes which are $1 \bmod 3$ $\left(\left(\frac{-3}{p_i}\right) = 1\right)$

The proofs of these Theorems are very similar to the proof that $n \in \mathbb{Z}_+$ can be written as $a^2 + b^2 \iff n = N^2 2^k \prod_{i=1}^{l} p_i$ $p_i \equiv 1 \bmod 4$. $\left(\left(\frac{-1}{p_i}\right) = 1\right)$

Steps in the proof

Use the rings $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$ for the first two theorems

The third theorem uses the ring $\mathcal{O}[\sqrt{-3}]$ rather than $\mathbb{Z}[\sqrt{-3}]$

because $\mathbb{Z}[\sqrt{-3}]$ is not a UFD and $\mathcal{O}[\sqrt{-3}]$ is.

(In fact $\mathcal{O}[\sqrt{-3}] = \mathbb{Z}[\omega]$, where $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$, so that $\omega^2 + \omega + 1 = 0$

Both $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{-2}]$ are UFD's and this is used.

$a + b\sqrt{2}$ prime in $\mathbb{Z}[\sqrt{2}]$ $\iff$ $a^2 - 2b^2$ prime in $\mathbb{Z}$

For $\Rightarrow$ this uses unique factorisation.

So $v(a+b\sqrt{2}) = |a^2 - 2b^2|$ $(a, b \in \mathbb{Z})$ is multiplicative.

So if $n \in \mathbb{Z}$ and $a+b\sqrt{2}$ prime in $\mathbb{Z}[\sqrt{2}]$

$a + b\sqrt{2} \mid n \Rightarrow a^2 - 2b^2 \mid n^2 \Rightarrow a^2 - 2b^2 \mid n$ (because $a^2 - 2b^2$ prime

$a^2 - 2b^2$ for integers a, b $\iff$ all prime divisors of n

So $n = a^2 - 2b^2$ have such an expression. (Similarly for $\mathbb{Z}[\sqrt{-2}]$ etc.)

But then, if p is a prime integer and $kp = a^2 - 2b^2$ for $a, b \in \mathbb{Z}$

and $k \in \mathbb{Z} \setminus \{0\}$, $p = a_1^2 - 2b_1^2$ for some $a_1, b_1 \in \mathbb{Z}$

$(-1 = 1^2 - 2 \times 1^2$ so kp has such an expression $\iff -kp$ does)

$kp = a^2 - 2b^2$ for some integer k and coprime a, b

$\iff a^2 \equiv 2b^2 \bmod p$ for a, b coprime to $p \iff x^2 \equiv 2 \bmod p$

for some integer x coprime to $p \iff \left(\frac{2}{p}\right) = 1$

Similarly $kp = a^2 + 2b^2$ for some $k \in \mathbb{Z} \setminus \{0\} \iff \left(\frac{-2}{p}\right) = 1 \ldots$

Examples

$n \in \mathbb{Z}_+$ written as $a^2 - 2b^2$.

Note: always infinitely many solutions because of the presence of rational units.

$2 = 2^2 - 2\times 1^2$ $\quad 4 = (2+\sqrt{2})^2(2-\sqrt{2})^2 = 6^2 - 2\times 4^2$

$7 = 5^2 - 2\times 3^2$ $\quad 17 = 5^2 - 2\times 2^2$ $\quad 31 = 9^2 - 2\times 5^2 \ldots$

$14 = 4^2 - 2\times 1^2$ $\quad 28 = 6^2 - 2\times 2^2$ $\quad 34 = 6^2 - 2\times 1^2 \ldots$

Example

An application of quadratic residue theory.

Recall $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \bmod 4$.

We will use this to show there are infinitely many primes which are $1 \bmod 4$.

Suppose there are only finitely many primes q_i, $1 \le i \le k$, which are $1 \bmod 4$.

Write $N = \prod_{i=1}^{k} q_i$

Consider $4N^2+1$. Let p be any prime dividing $4N^2+1$.

Then p is odd and $p \neq q_i$, $1 \le i \le k$ because $q_i \mid N$, $q_i \nmid 4N^2+1$.

$-1 \equiv 4N^2 \equiv (2N)^2 \bmod p$

So $\left(\frac{-1}{p}\right) = 1$ and $p \equiv 1 \bmod 4 \Rightarrow p = q_i$ for some i $\times$.