

# Solutions to Ireland, Rosen “A Classical Introduction to Modern Number Theory”

Richard Ganaye

September 9, 2023

## Chapter 9

**Ex. 9.1** If  $\alpha \in \mathbb{Z}[\omega]$ , show that  $\alpha$  is congruent to either 0, 1, or  $-1$  modulo  $1 - \omega$ .

*Proof.* Let  $\lambda = 1 - \omega$ , and  $\alpha = a + b\omega \in D = \mathbb{Z}[\omega]$ ,  $a, b \in \mathbb{Z}$ .

$\omega \equiv 1 \pmod{\lambda}$ , so  $\alpha \equiv a + b \pmod{\lambda}$ ,  $\alpha \equiv c$  with  $c = a + b \in \mathbb{Z}$ .

$c \equiv 0, 1, -1 \pmod{3}$ , and since  $\lambda \mid 3$ ,  $z \equiv 0, 1, -1 \pmod{\lambda}$ .

Every  $\alpha \in D$  is congruent to either 0, 1, or  $-1$  modulo  $\lambda = 1 - \omega$ .

The classes of 0, 1,  $-1$  in  $D/\lambda D$  are distinct. Indeed,  $1 \not\equiv -1 \pmod{\lambda}$ , if not  $\lambda \mid 2$ , so  $2 = \lambda\lambda'$ ,  $N(2) = N(\lambda)N(\lambda')$ , thus  $4 = 3N(\lambda')$ , so  $3 \mid 4$ , which is nonsense.

$\pm 1 \equiv 0 \pmod{\lambda}$  implies  $\lambda \mid 1$ , so  $\lambda$  would be a unit, in contradiction with  $\lambda$  prime.

So there exist exactly three classes modulo  $\lambda$  in  $D$  :  $|D/\lambda D| = 3 = N(\lambda)$ .

□

**Ex. 9.2** From now on we shall set  $D = \mathbb{Z}[\omega]$  and  $\lambda = 1 - \omega$ . For  $\mu$  in  $D$  show that we can write  $\mu = (-1)^a \omega^b \lambda^c \pi_1^{a_1} \pi_2^{a_2} \cdots \pi_t^{a_t}$ , where  $a, b, c$ , and the  $a_i$  are nonnegative integers and the  $\pi_i$  are primary primes.

*Proof.* Let  $S$  the set containing  $\lambda = 1 - \omega$  and all primary primes.

We show that

- (a) every prime in  $D$  is associate to a prime in  $S$ ,
- (b) no two primes in  $S$  are associate.

Let  $\pi$  be a prime in  $D$ . There are three cases.

- If  $N(\pi) = 3$ , then  $\pi$  is associate to  $\lambda \in S$ , thus  $\pi \in \{1 - \omega, -1\omega, -2 - \omega, 2 + \omega, 1 + 2\omega, -1 - 2\omega\}$ , and no associate of  $\lambda$  is primary.
- If  $N(\pi) = q^2$ , where  $q \equiv -1 \pmod{3}$ ,  $q > 0$ , is a rational prime, then  $\pi$  is associate to  $q$  (Proposition 9.1.2), and  $q$  is a primary prime. The primes associate to  $q$  are  $q, -q, \omega q, -\omega q, -q - \omega q, q + \omega q$ , so only  $q$  is primary.
- If  $N(\pi) = p$ , where  $p \equiv 1 \pmod{4}$ , then the proposition 9.1.4. shows that among the associates to  $\pi$  exactly one is primary.

Moreover, the norm of two primes belonging to two different cases are distinct, so two such primes are not associate.

By Theorem 3, Chapter 1, as  $D = \mathbb{Z}[\omega]$  is a principal ideal domain, every  $\mu \in D$  is of the form

$$\mu = u \prod_{\pi \in S} \pi^{e(\pi)},$$

where  $u$  is a unit, so  $u = (-1)^a \omega^b$ . Thus

$$\mu = (-1)^a \omega^b \lambda^c \pi_1^{a_1} \pi_2^{a_2} \cdots \pi_t^{a_t},$$

where the  $\pi$  are primary primes, and  $a, b, c$  and the  $a_i$  are nonnegative integers.  $\square$

**Ex. 9.3** Let  $\gamma$  a primary prime. To evaluate  $\chi_\gamma(\mu)$  we see, by Exercise 2, that it is enough to evaluate  $\chi_\gamma(-1), \chi_\gamma(\omega), \chi_\gamma(\lambda)$ , and  $\chi_\gamma(\pi)$ , where  $\pi$  is a primary prime. Since  $-1 = (-1)^3$  we have  $\chi_\gamma(-1) = 1$ . We now consider  $\chi_\gamma(\omega)$ . Let  $\gamma = a + b\omega$  and set  $a = 3m - 1$  and  $b = 3n$ . Show that  $\chi_\gamma(\omega) = \omega^{m+n}$ .

*Proof.* Let  $\gamma = a + b\omega = 3m - 1 + 3n\omega$ . Then  $\chi_\gamma(\omega) = \omega^{\frac{N(\gamma)-1}{3}}$  (remark (b) of Theorem 1).

$$\begin{aligned} N(\gamma) - 1 &= (3m - 1)^2 + (3n)^2 - 3n(3m - 1) - 1 \\ &= 9m^2 - 6m + 9n^2 - 9nm + 3n \\ \frac{N(\gamma) - 1}{3} &= 3m^2 - 2m + 3n^2 - 3nm + n \equiv n + m \pmod{3} \end{aligned}$$

Thus, for  $\gamma = a + b\omega = 3m - 1 + 3n\omega$ ,

$$\chi_\gamma(\omega) = \omega^{\frac{N(\gamma)-1}{3}} = \omega^{n+m}.$$

$\square$

**Ex. 9.4** (continuation) Show that  $\chi_\gamma(\omega) = 1, \omega$ , or  $\omega^2$  according to whether  $\gamma$  is congruent to 8, 2, or 5 modulo  $3\lambda$ . In particular, if  $q$  is a rational prime,  $q \equiv 2 \pmod{3}$ , then  $\chi_q(\omega) = 1, \omega$ , or  $\omega^2$  according to whether  $q \equiv 8, 2$ , or  $5 \pmod{9}$ . [Hint :  $\gamma = a + b\omega = -1 + 3(m + n\omega)$ , and so  $\gamma \equiv -1 + 3(m + n) \pmod{3\lambda}$ .]

*Proof.*  $\lambda = 1 - \omega$ , so  $\omega \equiv 1 \pmod{\lambda}$ . Thus

$$\begin{aligned} m + n\omega &\equiv m + n \pmod{\lambda} \\ 3(m + n\omega) &\equiv 3(m + n) \pmod{3\lambda} \\ \gamma &\equiv -1 + 3(m + n\omega) \equiv -1 + 3(m + n) \pmod{3\lambda} \end{aligned}$$

Moreover  $9 = 3\lambda\bar{\lambda} \equiv 0 \pmod{3\lambda}$ , thus  $\gamma$  is congruent modulo  $3\lambda$  to an integer between 0 and 8 of the form  $3k - 1$  :  $\gamma \equiv 8, 2$  or  $5 \pmod{3\lambda}$ .

By Ex. 9.3,  $\chi_\gamma(\omega) = 1 \iff m + n \equiv 0 \pmod{3}$ , and  $m + n \equiv 0 \pmod{3}$  implies  $m + n = 3k, k \in \mathbb{Z}$ , so  $\gamma \equiv -1 + 9k \equiv -1 \equiv 8 \pmod{3\lambda}$ .

Conversely, if  $\gamma \equiv 8 \equiv -1 \pmod{3\lambda}$ , then  $3\lambda \mid 3(m + n)$ , so  $\lambda \mid m + n$ , and  $N(\lambda) \mid N(m + n)$ ,  $3 \mid (m + n)^2$ , thus  $3 \mid m + n$ ,  $m + n \equiv 0 \pmod{3}$ , and so  $\chi_\gamma(\omega) = 1$ . The two other cases are similar, so we obtain

$$\begin{aligned}
\chi_\gamma(\omega) = 1 &\iff m+n \equiv 0 \pmod{3} \iff \gamma \equiv 8 \pmod{3\lambda}, \\
\chi_\gamma(\omega) = \omega &\iff m+n \equiv 1 \pmod{3} \iff \gamma \equiv 2 \pmod{3\lambda}, \\
\chi_\gamma(\omega) = \omega^2 &\iff m+n \equiv 2 \pmod{3} \iff \gamma \equiv 5 \pmod{3\lambda}.
\end{aligned}$$

If  $\gamma = q$  is a rational prime,  $q \equiv 8 \pmod{9}$  implies  $q \equiv 8 \pmod{3\lambda}$ , since  $3\lambda \mid 9 = 3\lambda\bar{\lambda}$ , thus  $\chi_q(\omega) = 1$ .

Conversely, if  $\chi_q(\omega) = 1$ , then  $q \equiv 8 \pmod{3\lambda}$ ,  $q - 8 = \mu(3\lambda)$ ,  $\mu \in D$ , therefore  $(q - 8)^2 = N(\mu)3^3$ ,  $3^3 \mid (q - 8)^2$ , thus  $3^2 \mid q - 8$  and so  $q \equiv 8 \pmod{9}$ . The two other cases are similar.

$$\begin{aligned}
\chi_q(\omega) = 1 &\iff q \equiv 8 \pmod{9}, \\
\chi_q(\omega) = \omega &\iff q \equiv 2 \pmod{9}, \\
\chi_q(\omega) = \omega^2 &\iff q \equiv 5 \pmod{9}.
\end{aligned}$$

□

**Ex. 9.5** In the text we stated Eisenstein's result  $\chi_\gamma(\lambda) = \omega^{2m}$ . Show that  $\chi_\gamma(3) = \omega^{2n}$ .

*Proof.* Here  $\gamma = (3m - 1) + 3n\omega$ .

Note that  $(1 - \omega)^2 = -3\omega$ , thus  $\chi_\gamma((1 - \omega)^2) = \chi_\gamma(-1)\chi_\gamma(3)\chi_\gamma(\omega)$ .

Using Eisenstein's result (see a proof in Ex.24-26),

$$\chi_\gamma((1 - \omega)^2) = \chi_\gamma(\lambda^2) = \chi_\gamma(\lambda)^2 = \omega^{4m} = \omega^m.$$

As  $-1 = (-1)^3$ ,  $\chi_\gamma(-1) = 1$ . Finally  $\chi_\gamma(\omega) = \omega^{m+n}$  by Exercise 9.3. Thus

$$\omega^m = \chi_\gamma(3)\omega^{m+n}, \quad \chi_\gamma(3) = \omega^{-n} = \omega^{2n}.$$

In conclusion,

$$\chi_\gamma(3) = \omega^{2n}.$$

□

**Ex. 9.6** Prove that

(a)  $\chi_\gamma(\lambda) = 1$  for  $\gamma \equiv 8, 8 + 3\omega, 8 + 6\omega \pmod{9}$ .

(b)  $\chi_\gamma(\lambda) = \omega$  for  $\gamma \equiv 5, 5 + 3\omega, 5 + 6\omega \pmod{9}$ .

(c)  $\chi_\gamma(\lambda) = \omega^2$  for  $\gamma \equiv 2, 2 + 3\omega, 2 + 6\omega \pmod{9}$ .

*Proof.* Here  $\gamma = -1 + 3(m + n\omega)$  is a primary prime, and  $\chi_\gamma(\lambda) = \omega^{2m}$ .

$$\begin{aligned}
\chi_\gamma(\lambda) = 1 &\iff m \equiv 0 \pmod{3} \Rightarrow \gamma \equiv 8 + 3n\omega \pmod{9} \Rightarrow \gamma \equiv 8, 8 + 3\omega, 8 + 6\omega \pmod{9} \\
\chi_\gamma(\lambda) = \omega &\iff m \equiv 2 \pmod{3} \Rightarrow \gamma \equiv 5 + 3n\omega \pmod{9} \Rightarrow \gamma \equiv 5, 5 + 3\omega, 5 + 6\omega \pmod{9} \\
\chi_\gamma(\lambda) = \omega^2 &\iff m \equiv 1 \pmod{3} \Rightarrow \gamma \equiv 2 + 3n\omega \pmod{9} \Rightarrow \gamma \equiv 2, 2 + 3\omega, 2 + 6\omega \pmod{9}
\end{aligned}$$

As  $\chi_\gamma(\lambda) \in \{1, \omega, \omega^2\}$ , these 9 cases are the only possibilities. Moreover these 9 cases are mutually exclusive, since 9 doesn't divide any difference. Thus the reciprocals are true.

$$\begin{aligned}\chi_\gamma(\lambda) = 1 &\iff \gamma \equiv 8, 8 + 3\omega, 8 + 6\omega \text{ [9]} \\ \chi_\gamma(\lambda) = \omega &\iff \gamma \equiv 5, 5 + 3\omega, 5 + 6\omega \text{ [9]} \\ \chi_\gamma(\lambda) = \omega^2 &\iff \gamma \equiv 2, 2 + 3\omega, 2 + 6\omega \text{ [9]}\end{aligned}$$

□

**Ex. 9.7** Find primary primes associate to  $1 - 2\omega$ ,  $-7 - 3\omega$ , and  $3 - \omega$ .

*Proof.* :

- $(1 - 2\omega)\omega = 2 + 3\omega \equiv 2 \pmod{3}$ , so  $2 + 3\omega$  is primary, and associate to  $1 - 2\omega$ .  
 $N(2 + 3\omega) = 7$  and 7 is a rational prime, thus  $2 + 3\omega$  is a primary prime.
- $-7 - 3\omega \equiv 2 \pmod{3}$ .  
 $N(-7 - 3\omega) = 37$  and 37 is a rational prime, thus  $-7 - 3\omega$  is a primary prime.
- $(3 - \omega)\omega^2 = -4 - 3\omega \equiv 2 \pmod{3}$ , so  $-4 - 3\omega$  is primary, and associate to  $3 - \omega$ .  
 $N(-4 - 3\omega) = 13$  and 13 is a rational prime, thus  $-4 - 3\omega$  is a primary prime.

□

**Ex. 9.8** Factor the following numbers into primes in  $D$  : 7, 21, 45, 22, and 143.

*Proof.*  $7 = N(2 + 3\omega)$ , thus  $7 = (2 + 3\omega)(2 + 3\omega^2) = (2 + 3\omega)(-1 - 3\omega)$ , where  $2 + 3\omega$  and  $-1 - 3\omega$  are primes in  $D$ , since their norm is a prime integer. Since these primes are primary, they are not associate.

$$21 = 3 \times 7 = -\omega^2 \lambda^2 (2 + 3\omega)(-1 - 3\omega) \text{ since } 3 = -\omega^2(1 - \omega)^2.$$

$$45 = 3^2 \times 5 = \omega \lambda^4 5, \text{ where } 5 \equiv 2 \pmod{3} \text{ is a primary prime in } D.$$

$$22 = 2 \times 11, \text{ where 2 and 11 are primes in } D.$$

$$143 = 11 \times 13 = 11(-4 - 3\omega)(-4 - 3\omega^2) = 11(-4 - 3\omega)(-1 + 3\omega).$$

□

**Ex. 9.9** Show that  $\bar{\alpha} \neq 0$ , the residue class of  $\alpha$ , is a cube in the field  $D/\pi D$  iff  $\alpha^{(N\pi-1)/3} \equiv 1 \pmod{\pi}$ . Conclude that there are  $(N\pi - 1)/3$  cubes in  $(D/\pi D)^*$ .

Solution 1:

*Proof.* Let  $\pi$  be a prime in  $D$ ,  $N\pi \neq 3$ , and  $\alpha \in D, \pi \nmid \alpha$ .

$\bar{\alpha}$  is a cube in  $(D/\pi D)^*$

$$\iff x^3 \equiv \alpha \pmod{\pi} \text{ has a solution in } D$$

$$\iff \chi_\pi(\alpha) = 1 \quad (\text{by Prop. 9.3.3(a)})$$

$$\iff \alpha^{\frac{N\pi-1}{3}} \equiv 1 \pmod{\pi}$$

$$\iff \bar{\alpha}^{\frac{N\pi-1}{3}} = \bar{1}.$$

The cubes in  $(D/\pi D)^*$  are then the roots of the polynomial  $f(x) = x^{\frac{N\pi-1}{3}} - \bar{1}$  in  $D/\pi D$ .

Let  $q$  be the cardinal of the field  $D/\pi D$ . Since  $q = |D/\pi D| = N\pi$ ,  $\frac{N\pi-1}{3} \mid q-1$ ,  $f(x) \mid x^{q-1} - 1 \mid x^q - x$ . By Corollary 2 of Proposition 7.1.1,  $f$  has  $\deg(f) = \frac{N\pi-1}{3}$  roots. Conclusion: there are exactly  $\frac{N\pi-1}{3}$  cubes in  $(D/\pi D)^*$ .  $\square$

Solution 2:

*Proof.* Let  $\varphi : (D/\pi D)^* \rightarrow (D/\pi D)^*$  be the group homomorphism defined by  $\varphi(x) = x^3$ . Then  $\text{im}(\varphi)$  is the set of cubes in  $(D/\pi D)^*$ .

The equation  $x^3 = \bar{1}$  has three distinct solutions  $\bar{1}, \bar{\omega}, \bar{\omega}^2$  in  $D/\pi D$  if  $N\pi \neq 3$  (see the demonstration of Proposition 9.3.1).

Thus  $\ker(\varphi) = \{\bar{1}, \bar{\omega}, \bar{\omega}^2\}$  and  $|\ker(\varphi)| = 3$ . Therefore  $|\text{im}(\varphi)| = |(D/\pi D)^*|/|\ker(\varphi)| = (N\pi - 1)/3$ . There exist exactly  $\frac{N\pi-1}{3}$  cubes in  $(D/\pi D)^*$ .  $\square$

Note: if  $N\pi = 3$ , that is to say, if  $\pi$  is associate to  $1 - \omega$ ,  $D/\pi D = \{\bar{0}, \bar{1}, \bar{2}\}$ . As  $\bar{1}^3 = \bar{1}, \bar{2}^3 = \bar{2}$ , all the elements of  $(D/\pi D)^*$  are cubes.

**Ex. 9.10** What is the factorisation of  $x^{24} - 1$  in  $D/5D$ .

*Proof.*  $|(D/5D)^*| = N(5) - 1 = 24$ , thus  $x^{24} - 1 = \prod_{\alpha \in (D/5D)^*} (x - \alpha)$ .

(where the  $\alpha \in (D/5D)^*$  are of the form  $\alpha = a + b[\omega]$ ,  $0 \leq a < 5, 0 \leq b < 5, (a, b) \neq (0, 0)$ ).  $\square$

**Ex. 9.11** How many cubes are there in  $D/5D$  ?

*Proof.* By Exercise 9.9, there exist  $(N(5) - 1)/3 = 8$  cubes in  $(D/5D)^*$  (and  $0 = 0^3$  is a cube).  $\square$

**Ex. 9.12** Show that  $\omega\lambda$  has order 8 in  $D/5D$  and that  $\omega^2\lambda$  has order 24. [Hint : Show first that  $(\omega\lambda)^2$  has order 4.]

*Proof.* If  $\alpha = (\omega\lambda)^2$ , then

$$\alpha = (\omega\lambda)^2 = \omega^2(1 - \omega)^2 = \omega^2(1 + \omega^2 - 2\omega) = -3\omega^3 = -3.$$

So  $\alpha^2 = 9 \equiv -1 \pmod{5}$ ,  $\alpha^4 \equiv 1 \pmod{5}$  and  $\alpha^2 \not\equiv 1 \pmod{5}$ , thus the class of  $\alpha = (\omega\lambda)^2$  has order 4 in  $(D/5D)^*$ , and this implies that  $\omega\lambda$  has order 8.

Let  $\beta = \omega^2\lambda$ .  $|(D/5D)^*| = 24$ , thus  $[\beta]^{24} = 1$  (where  $[\beta]$  is the class of  $\beta$  in  $D/5D$ ).

To verify that  $[\beta]$  has order 24, it is sufficient to show that  $[\beta]^8 \neq 1, [\beta]^{12} \neq 1$ .

$$\beta^8 = \omega^{16}\lambda^8 = \omega\lambda^8 = (\omega\lambda)^8\omega^2 \equiv \omega^2 \not\equiv 1 \pmod{5}.$$

$$\beta^{12} = (\omega^2\lambda)^{12} = \lambda^{12} = (\omega\lambda)^{12} \equiv (\omega\lambda)^4 \equiv -1 \pmod{5} \text{ (since } (\omega\lambda) \text{ has order 8 in } D/5D).$$

Conclusion:  $\omega\lambda$  has order 8,  $\omega\lambda^2$  has order 24 in  $(D/5D)^*$ .  $\square$

**Ex. 9.13** Show that  $\pi$  is a cube in  $D/5D$  iff  $\pi \equiv 1, 2, 3, 4, 1 + 2\omega, 2 + 4\omega, 3 + \omega, \text{ or } 4 + 3\omega \pmod{5}$ .

*Proof.* Let  $\pi \in D, [\pi] \neq 0$ . Then  $[\pi]$  is a cube in  $D/5D$  iff  $[\pi]^{(q^2-1)/3} = 1$ , with  $q = 5$ , namely  $[\pi]^8 = 1$  (Prop. 7.1.2, where  $3 \mid q^2 - 1 = 24 = |(D/5D)^*|$ ).

By Exercise 9.12, the class of  $\gamma = \omega\lambda$  has order 8, thus the 8 elements  $[\gamma]^k, 0 \leq k \leq 7$  are distinct roots of the polynomial  $x^8 - 1$ , which has at most 8 roots. Therefore the subgroup of cubes in  $(D/5D)^*$  is

$$\{1, [\gamma], [\gamma]^2, \dots, [\gamma]^7\}.$$

$\gamma = \omega(1 - \omega) = \omega + 1 + \omega = 1 + 2\omega$ , so

$$\begin{aligned} \gamma^0 &= 1 \\ \gamma^1 &= 1 + 2\omega \\ \gamma^2 &\equiv -3 \equiv 2 \pmod{5} && (\text{Ex. 9.12}) \\ \gamma^3 &= -3 - 6\omega \equiv 2 + 4\omega \pmod{5} \\ \gamma^4 &\equiv -1 \equiv 4 \pmod{5} \\ \gamma^5 &\equiv -1 - 2\omega \equiv 4 + 3\omega \pmod{5} \\ \gamma^6 &\equiv 3 \pmod{5} \\ \gamma^7 &\equiv 3 + 6\omega \equiv 3 + \omega \pmod{5} \end{aligned}$$

Conclusion: If  $\pi \not\equiv 0 \pmod{5}$ ,  $\pi \equiv \alpha^3 \pmod{5}, \alpha \in D$  iff

$$\pi \equiv 1, 2, 3, 4, 1 + 2\omega, 2 + 4\omega, 3 + \omega, 4 + 3\omega \pmod{5}.$$

□

**Ex. 9.14** For which primes  $\pi \in D$  is  $x^3 \equiv 5 \pmod{\pi}$  solvable?

*Proof.* If  $\pi$  is associate to 5, then  $5^3 \equiv 0 \equiv 5 \pmod{\pi}$ , so  $x^3 \equiv 5 \pmod{\pi}$  is solvable.

If  $\pi$  is a primary prime not associate to 5, the Law of Cubic Reciprocity gives

$$\begin{aligned} 5 \equiv x^3 \pmod{\pi}, x \in D &\iff \chi_\pi(5) = 1 \\ &\iff \chi_5(\pi) = 1 \\ &\iff \pi \text{ is a cube in } D/5D \\ &\iff \pi \equiv 1, 2, 3, 4, 1 + 2\omega, 2 + 4\omega, 3 + \omega, 4 + 3\omega \pmod{5} \end{aligned}$$

(see Ex. 9.13)

Conclusion: the equation  $5 \equiv x^3 \pmod{\pi}, x \in D$  is solvable iff the primary prime associate to  $\pi$  is congruent modulo 5 to  $1, 2, 3, 4, 1 + 2\omega, 2 + 4\omega, 3 + \omega, 4 + 3\omega$  (or 0).

Examples:

- $q = 23$  is a primary prime congruent to 3 modulo 5, thus the equation  $x^3 \equiv 5 \pmod{23}$  has a solution  $x \in D$  ( $x = 19$ ).

- $-4 - 3\omega$  is the primary prime associate to the prime  $3 - \omega$ , and  $-4 - 3\omega \equiv 1 + 2\omega \pmod{5}$ , thus the equation  $x^3 \equiv 5 \pmod{3 - \omega}$  has a solution  $a + b\omega \in \mathbb{Z}[\omega]$ .

Indeed,  $7^3 \equiv 8^3 \equiv 11^3 \equiv 5 \pmod{13}$ , and  $3 - \omega \mid 13$ , so  $7^3 \equiv 8^3 \equiv 11^3 \equiv 5 \pmod{3 - \omega}$ . □

**Ex. 9.15** Suppose that  $p \equiv 1 \pmod{3}$  and that  $p = \pi\bar{\pi}$ , where  $\pi$  is a primary prime in  $D$ . Show that  $x^3 \equiv a \pmod{p}$  is solvable in  $\mathbb{Z}$  iff  $\chi_\pi(a) = 1$ . We assume that  $a \in \mathbb{Z}$ .

*Proof.* Since  $\pi \mid p$ , if  $x^3 \equiv a \pmod{p}$ ,  $x \in \mathbb{Z}$ , then  $x^3 \equiv a \pmod{\pi}$ , thus  $\chi_\pi(a) = 1$ .

Conversely, suppose that  $\chi_\pi(a) = 1$ . Then the equation  $y^3 \equiv a \pmod{\pi}$  has a solution  $y = u + v\omega$ ,  $u, v \in \mathbb{Z}$ . Moreover, the class of  $y$  has a representative  $x \in \mathbb{Z}$  modulo  $\pi$  (see the proof of Proposition 9.2.1) :

$$y \equiv x \pmod{\pi}, x \in \mathbb{Z}.$$

So  $x^3 \equiv a \pmod{\pi}$  has a solution  $x \in \mathbb{Z}$ .

Thus  $\pi \mid x^3 - a$ ,  $N(\pi) = p \mid (x^3 - a)^2$ , therefore  $p \mid x^3 - a$  in  $\mathbb{Z}$ , and so  $x^3 \equiv a \pmod{p}$ .

Conclusion: if  $p \equiv 1 \pmod{3}$ ,  $p = \pi\bar{\pi}$ , where  $\pi$  is a primary prime, and  $a \in \mathbb{Z}$ ,

$$\exists x \in \mathbb{Z}, x^3 \equiv a \pmod{p} \iff \chi_\pi(a) = 1.$$

In other words,  $x^3 \equiv a \pmod{\pi}$  is solvable in  $D$  iff it is solvable in  $\mathbb{Z}$ . □

**Ex. 9.16** Is  $x^3 \equiv 2 - 3\omega \pmod{11}$  solvable? Since  $D/11D$  has 121 elements this is hard to resolve by straightforward checking. Fill in the details of the following proof that it is not solvable.  $\chi_\pi(2 - 3\omega) = \chi_{2-3\omega}(11)$  and so we shall have a solution iff  $x^3 \equiv 11 \pmod{2 - 3\omega}$  is solvable. This congruence is solvable iff  $x^3 \equiv 11 \pmod{7}$  is solvable in  $\mathbb{Z}$ . However,  $x^3 \equiv a \pmod{7}$  is solvable in  $\mathbb{Z}$  iff  $a \equiv 1$  or  $6 \pmod{7}$ .

Warning: false sentence, since

$$N(2 - 3\omega) = (2 - 3\omega)(2 - 3\omega^2) = 4 + 9 - 6(\omega + \omega^2) = 4 + 9 + 6 = 19 \text{ (and not 7!)}.$$

*Proof.* Since 19 is a rational prime, and since  $\pi = 2 - 3\omega$  and 11 are primary primes, by the Law of Cubic Reciprocity, and by Exercise 9.15 (with  $p = 11 \equiv 1 \pmod{3}$ ),

$$\begin{aligned} \exists x \in D, 2 - 3\omega \equiv x^3 [11] &\iff \chi_{11}(2 - 3\omega) = 1 \\ &\iff \chi_{2-3\omega}(11) = 1 \\ &\iff \exists x \in D, x^3 \equiv 11 [2 - 3\omega] \\ &\iff \exists x \in \mathbb{Z}, x^3 \equiv 11 [19] \end{aligned}$$

Moreover, by Proposition 7.1.2 (with  $p = 19$ ,  $d = (p - 1) \wedge 3 = 3$ ,  $(p - 1)/d = 6$ ),

$$\exists x \in \mathbb{Z}, x^3 \equiv 11 [19] \iff 11^6 \equiv 1 \pmod{19},$$

which is true :  $11^6 = 121^3 = (19 \times 6 + 7)^3 \equiv 49 \times 7 \equiv 11 \times 7 \equiv 77 \equiv 1 [19]$ .

Conclusion: there exists  $x \in D$  such that  $2 - 3\omega \equiv x^3 \pmod{11}$ .

With some computer code, we find a solution  $x = 1 + 8\omega$  (and its associates  $\omega^2 x = 7 - \omega$ ,  $\omega x = -8 - 7\omega \equiv 3 + 4\omega \pmod{11}$ ) :

$$x^3 = (1 + 8\omega)^3 = 321 - 168\omega \equiv 2 - 3\omega \pmod{11}.$$

□

Note: The sentence becomes true if we replace  $2 - 3\omega$  by the primary prime  $2 + 3\omega$ . Since  $N(2 + 3\omega) = 7$ , with the same reasoning,

$$\begin{aligned}\exists x \in D, 2 + 3\omega \equiv x^3 \pmod{11} &\iff \chi_{2+3\omega}(11) = 1 \\ &\iff \exists x \in D, x^3 \equiv 11 \pmod{2 + 3\omega} \\ &\iff \exists x \in \mathbb{Z}, x^3 \equiv 11 \equiv 4 \pmod{7} \\ &\iff 4^2 \equiv 1 \pmod{7}\end{aligned}$$

but  $4^2 \equiv 2 \not\equiv 1 \pmod{7}$ , so the equation  $x^3 \equiv 2 + 3\omega \pmod{11}$  is not solvable.

( $x^3 \equiv a \pmod{11}$  is solvable in  $\mathbb{Z}$  iff  $a^{\frac{7-1}{3}} = a^2 \equiv 1 \pmod{7}$  iff  $a \equiv \pm 1 \pmod{7}$ .)

**Ex. 9.17** An element  $\gamma \in D$  is called primary if  $\gamma \equiv 2 \pmod{3}$ . If  $\gamma$  and  $\rho$  are primary, show that  $-\gamma\rho$  is primary. If  $\gamma$  is primary, show that  $\gamma = \pm\gamma_1\gamma_2 \dots \gamma_t$ , where the  $\gamma_i$  are (not necessarily distinct) primary primes.

*Proof.* If  $\gamma \equiv 2, \rho \equiv 2 \pmod{3}$ , then  $-\gamma\rho \equiv -2 \times 2 \equiv 2 \pmod{3}$ , so  $-\gamma\rho$  is primary.

By Ex. 9.2,  $\gamma$  can be written

$$\gamma = (-1)^a \omega^b \lambda^c \pi_1^{a_1} \dots \pi_t^{a_t},$$

where  $\pi_i \equiv 2 \pmod{3}, a \in \{0, 1\}, b \in \{0, 1, 2\}$ .

As  $\pi_i \equiv -1 \pmod{3}$ , and  $\gamma \equiv -1 \pmod{3}$ , we obtain  $\omega^b \lambda^c \equiv \pm 1 \pmod{3}$ . We prove that  $b = c = 0$ .

Note that  $\lambda^2 = (1 - \omega)^2 = -3\omega \equiv 0 \pmod{3}$ . If  $c \geq 2$ , we would obtain  $\gamma \equiv 0 \pmod{3}$ , in contradiction with the hypothesis, thus  $c = 0$  or  $c = 1$ .

If  $c = 1$ ,

$$\omega^b \lambda^c \in \{1 - \omega, \omega(1 - \omega), \omega^2(1 - \omega)\} = \{1 - \omega, 1 + 2\omega, -2 - \omega\}.$$

Since  $1 - \omega \not\equiv \pm 1, 1 + 2\omega \not\equiv \pm 1, -2 - \omega \not\equiv \pm 1 \pmod{3}$ , this is impossible, so  $c = 0$ .

Then  $\omega^b \equiv \pm 1 \pmod{3}$ , where  $\omega^b \in \{1, \omega, -1 - \omega\}$ . Since  $\omega \not\equiv \pm 1 \pmod{3}$ , and  $-1 - \omega \not\equiv \pm 1 \pmod{3}$ , then  $\omega^b = 1, 0 \leq b \leq 2$ , thus  $b = 0$ .

Finally,  $\gamma = (-1)^a \pi_1^{a_1} \dots \pi_t^{a_t}$ .

Conclusion: Every primary  $\gamma \in D$  is under the form

$$\gamma = \pm\gamma_1\gamma_2 \dots \gamma_t,$$

where the  $\gamma_i$  are primary primes. □

**Ex. 9.18** (continuation) If  $\gamma = \pm\gamma_1\gamma_2 \dots \gamma_t$  is a primary decomposition of the primary element  $\gamma$ , define  $\chi_\gamma(\alpha) = \chi_{\gamma_1}(\alpha)\chi_{\gamma_2}(\alpha) \dots \chi_{\gamma_t}(\alpha)$ . Prove that  $\chi_\gamma(\alpha) = \chi_\gamma(\beta)$  if  $\alpha \equiv \beta \pmod{\gamma}$  and  $\chi_\gamma(\alpha\beta) = \chi_\gamma(\alpha)\chi_\gamma(\beta)$ . If  $\rho$  is primary, show that  $\chi_\rho(\alpha)\chi_\gamma(\alpha) = \chi_{-\rho\gamma}(\alpha)$ .

*Proof.* If  $\alpha \equiv \beta \pmod{\gamma}$ , then  $\alpha \equiv \beta \pmod{\gamma_i}, 1 \leq i \leq t$ , so  $\chi_{\gamma_i}(\alpha) = \chi_{\gamma_i}(\beta)$ , thus  $\chi_\gamma(\alpha) = \chi_\gamma(\beta)$ .

By Proposition 9.3.3,

$$\begin{aligned}\chi_\gamma(\alpha\beta) &= \chi_{\gamma_1}(\alpha\beta)\chi_{\gamma_2}(\alpha\beta) \dots \chi_{\gamma_t}(\alpha\beta) \\ &= \chi_{\gamma_1}(\alpha)\chi_{\gamma_2}(\alpha) \dots \chi_{\gamma_t}(\alpha)\chi_{\gamma_1}(\beta)\chi_{\gamma_2}(\beta) \dots \chi_{\gamma_t}(\beta) \\ &= \chi_\gamma(\alpha)\chi_\gamma(\beta)\end{aligned}$$



Finally, if  $\rho = \pm\rho_1\rho_2\cdots\rho_l$  is primary, then  $-\rho\gamma = \pm\rho_1\rho_2\cdots\rho_l\gamma_1\gamma_2\cdots\gamma_t$  is primary by Ex. 9.17, therefore

$$\chi_{-\rho\gamma}(\alpha) = (\chi_{\rho_1}\chi_{\rho_2}\cdots\chi_{\rho_l}\chi_{\gamma_1}\chi_{\gamma_2}\cdots\chi_{\gamma_t})(\alpha) = \chi_{\rho}(\alpha)\chi_{\gamma}(\alpha).$$

□

Note: The unit  $-1$  is primary by definition, and  $-1$  is the opposite of the empty product, so for all  $\alpha$  in  $D$ ,  $\chi_{-1}(\alpha) = 1$  by definition. The result of the exercises remain true if we accept the unit  $-1$  as a primary element.

**Ex. 9.19** Suppose that  $\gamma = A + B\omega$  is primary and that  $A = 3M - 1$  and  $B = 3N$ . Prove that  $\chi_{\gamma}(\omega) = \omega^{M+N}$  and that  $\chi_{\gamma}(\lambda) = \omega^{2M}$ .

*Proof.* We verify first that if  $\gamma = -\gamma_1\gamma_2$ , with

$$\begin{aligned}\gamma &= A + B\omega, & A &= 3M - 1, & B &= 3N, \\ \gamma_1 &= A_1 + B_1\omega, & A_1 &= 3M_1 - 1, & B_1 &= 3N_1, \\ \gamma_2 &= A_2 + B_2\omega, & A_2 &= 3M_2 - 1, & B_2 &= 3N_2,\end{aligned}$$

then  $M \equiv M_1 + M_2 \pmod{3}$ ,  $N \equiv N_1 + N_2 \pmod{3}$ .

$$-\gamma_1\gamma_2 = -A_1A_2 + B_1B_2 + (-A_1B_2 - A_2B_1 + B_1B_2)\omega = A + B\omega,$$

therefore

$$3M - 1 = A = -A_1A_2 + B_1B_2 \equiv 3(M_1 + M_2) - 1 \pmod{9},$$

thus  $M \equiv M_1 + M_2 \pmod{3}$ .

$$3N = B = -A_1B_2 - A_2B_1 + B_1B_2 \equiv 3(N_1 + N_2) \pmod{9},$$

thus  $N \equiv N_1 + N_2 \pmod{3}$ .

By induction, if  $\gamma = \pm\gamma_1\gamma_2\cdots\gamma_t = (-1)^{t-1}\gamma_1\gamma_2\cdots\gamma_t$ , where  $\gamma_i = A_i + B_i\omega$ ,  $A_i = 3M_i - 1$ ,  $B_i = 3N_i$ , then

$$M \equiv M_1 + \cdots + M_t \pmod{3}, N \equiv N_1 + \cdots + N_t \pmod{3}.$$

By Exercise 9.3,

$$\begin{aligned}\chi_{\gamma}(\omega) &= \chi_{\gamma_1}(\omega) \cdots \chi_{\gamma_t}(\omega) \\ &= \omega^{M_1+N_1} \cdots \omega^{M_t+N_t} \\ &= \omega^{(M_1+\cdots+M_t)+(N_1+\cdots+N_t)} \\ &= \omega^{M+N},\end{aligned}$$

and by Eisenstein's result,

$$\begin{aligned}\chi_{\gamma}(\lambda) &= \chi_{\gamma_1}(\lambda) \cdots \chi_{\gamma_t}(\lambda) \\ &= \omega^{2M_1} \cdots \omega^{2M_t} \\ &= \omega^{2(M_1+\cdots+M_t)} \\ &= \omega^{2M}.\end{aligned}$$

Conclusion: if  $\gamma = 3M - 1 + 3N\omega$ , then

$$\chi_{\gamma}(\omega) = \omega^{M+N}, \chi_{\gamma}(\lambda) = \omega^{2M}.$$

□

**Ex. 9.20** If  $\gamma$  and  $\rho$  are primary, show that  $\chi_\gamma(\rho) = \chi_\rho(\gamma)$ .

Important note: The following solution assumes that  $\chi_{\pi_2}(\pi_1) = \chi_{\pi_1}(\pi_2)$  for any pair  $\pi_1, \pi_2$  of primary primes. But Theorem 1 uses the hypothesis  $N(\pi_1) \neq N(\pi_2)$  to prove Cubic Reciprocity.

We can complete the proof in the case where  $N(\pi_1) = N(\pi_2)$ . Since  $\pi_1, \pi_2$  are primary primes, then  $\pi_1 = \pi_2$  or  $\pi_1 = \overline{\pi_2}$ .

In the case  $\pi_1 = \pi_2$ , then  $\chi_{\pi_2}(\pi_1) = 0 = \chi_{\pi_1}(\pi_2)$ .

To prove that  $\left(\frac{\overline{\pi}}{\pi}\right) = \left(\frac{\pi}{\overline{\pi}}\right)$ , we begin with a particular case of the proposition:

**Lemma.** Let  $n \in \mathbb{Z}$  be a primary element in  $A$ , and let  $\pi$  be a primary prime such that  $N(\pi) = p \equiv 1 \pmod{3}$ . Then

$$\left(\frac{n}{\pi}\right)_3 = \left(\frac{\pi}{n}\right)_3.$$

*Proof.* If  $p \mid n$ , then  $\left(\frac{n}{\pi}\right)_3 = 0 = \left(\frac{\pi}{n}\right)_3$ . Now we assume that  $p \nmid n$ .

The decomposition of  $n$  is of the form

$$\begin{aligned} n &= \pm p_1 \cdots p_s q_1 \cdots q_r \quad (p_i \equiv 1 \pmod{3}, q_j \equiv -1 \pmod{3}) \\ &= \pm \pi_1 \overline{\pi_1} \cdots \pi_s \overline{\pi_s} q_1 \cdots q_r, \end{aligned}$$

where  $\pi_i, \overline{\pi_i} (1 \leq i \leq s)$  and  $q_j (1 \leq j \leq r)$  are primary prime.

Since  $N(\pi_i) = p \neq p_i$  and  $N(\pi) = p \neq N(q_j) = q_j^2$ , Theorem 1 shows that

$$\begin{aligned} \left(\frac{n}{\pi}\right)_3 &= \left(\frac{\pi_1}{\pi}\right)_3 \left(\frac{\overline{\pi_1}}{\pi}\right)_3 \cdots \left(\frac{\pi_s}{\pi}\right)_3 \left(\frac{\overline{\pi_s}}{\pi}\right)_3 \left(\frac{q_1}{\pi}\right)_3 \cdots \left(\frac{q_r}{\pi}\right)_3 \\ &= \left(\frac{\pi}{\pi_1}\right)_3 \left(\frac{\pi}{\overline{\pi_1}}\right)_3 \cdots \left(\frac{\pi}{\pi_s}\right)_3 \left(\frac{\pi}{\overline{\pi_s}}\right)_3 \left(\frac{\pi}{q_1}\right)_3 \cdots \left(\frac{\pi}{q_r}\right)_3 \\ &= \left(\frac{\pi}{n}\right)_3. \end{aligned}$$

□

We can now remove the useless hypothesis  $N(\pi_1) \neq N(\pi_2)$  in Theorem 1.

**Proposition.** Let  $\pi_1, \pi_2$  be primary primes. Then

$$\left(\frac{\pi_2}{\pi_1}\right)_3 = \left(\frac{\pi_1}{\pi_2}\right)_3.$$

*Proof.* By theorem 1, it remains only the case where  $N(\pi_1) = N(\pi_2)$ .

If  $\pi_1 = \pi_2$ , then  $\left(\frac{\pi_2}{\pi_1}\right)_3 = \left(\frac{\pi_1}{\pi_2}\right)_3 = 0$ .

If  $\pi_1 \neq \pi_2$ , since  $\pi_1$  et  $\pi_2$  are primary, then  $\pi_1, \pi_2$  are primes such that  $N(\pi_1) = N(\pi_2) = p \equiv 1 \pmod{3}$ , and  $\pi_2 = \overline{\pi_1}$ . Writing  $\pi = \pi_1$ , it is sufficient to prove

$$\left(\frac{\overline{\pi}}{\pi}\right)_3 = \left(\frac{\pi}{\overline{\pi}}\right)_3.$$

We use the “Evans’ trick” (see [Lemmermayer, Reciprocity Laws p. 215]). The element  $n = -(\pi + \bar{\pi})$  is a rational integer, which is primary. The Lemma gives then

$$\begin{aligned}
\left(\frac{\bar{\pi}}{\pi}\right)_3 &= \left(\frac{\pi + \bar{\pi}}{\pi}\right)_3 \\
&= \left(\frac{-\pi - \bar{\pi}}{\pi}\right)_3 \\
&= \left(\frac{\pi}{-\pi - \bar{\pi}}\right)_3 \\
&= \left(\frac{-\bar{\pi}}{-\pi - \bar{\pi}}\right)_3 \\
&= \left(\frac{\bar{\pi}}{-\pi - \bar{\pi}}\right)_3 \\
&= \left(\frac{-\pi - \bar{\pi}}{\bar{\pi}}\right)_3 \\
&= \left(\frac{-\pi}{\bar{\pi}}\right)_3 \\
&= \left(\frac{\pi}{\bar{\pi}}\right)_3
\end{aligned}$$

□

We can now give the solution of Exercise 9.20.

*Proof.*  $\rho, \gamma$  are written

$$\begin{aligned}
\rho &= \pm \rho_1 \rho_2 \cdots \rho_l, \\
\gamma &= \pm \gamma_1 \gamma_2 \cdots \gamma_m,
\end{aligned}$$

where  $\rho_i, \gamma_i$  are primary primes. By the law of Cubic Reciprocity, we obtain

$$\begin{aligned}
\chi_\gamma(\rho) &= \prod_{j=1}^m \chi_{\gamma_j}(\rho) \\
&= \prod_{j=1}^m \prod_{i=1}^l \chi_{\gamma_j}(\rho_i) \\
&= \prod_{i=1}^l \prod_{j=1}^m \chi_{\gamma_j}(\rho_i) \\
&= \prod_{i=1}^l \prod_{j=1}^m \chi_{\rho_i}(\gamma_j) \\
&= \prod_{i=1}^l \chi_{\rho_i}(\gamma) \\
&= \chi_\rho(\gamma).
\end{aligned}$$

(if  $\gamma = -1$ , or  $\rho = -1$ , some products are empty, but the result remains true:  $\chi_{-1}(\rho) = 1 = \chi_\rho(-1)$ .)

□

**Ex. 9.21** If  $\gamma$  is primary, show that there are infinitely many primary primes  $\pi$  such that  $x^3 \equiv \gamma \pmod{\pi}$  is not solvable. Show also that there are infinitely many primary primes  $\pi$  such that  $x^3 \equiv \omega \pmod{\pi}$  is not solvable and the same for  $x^3 \equiv \lambda \pmod{\pi}$ . (Hint: Imitate the proof of Theorem 3 of Chapter 5.)

*Proof.* a) As some primary elements of  $D$  may be cubes, by example  $53 + 36\omega = (-1 + 3\omega)^3$ , we must of course suppose that  $\gamma$  is not the cube of some element of  $D$  (in the contrary case  $x^3 \equiv \gamma \pmod{\pi}$  is solvable for all prime  $\pi$ ).

Note first that for all primes  $\pi$  in  $D$ , there exists  $\sigma \in D$  such that  $\chi_\pi(\sigma) = \omega$ . Indeed, there exist  $(N\pi - 1)/3$  cubes in  $(D/\pi D)^*$ , which has  $N\pi - 1$  elements, so there exists an element  $\bar{\tau} \in (D/\pi D)^*$  which is not a cube, therefore there exists  $\tau \in D$  such that  $\chi_\pi(\tau) \neq 1$ . If  $\chi_\pi(\tau) = \omega$ , we put  $\sigma = \tau$  and if  $\chi_\pi(\tau) = \omega^2$ , we put  $\sigma = \tau^2$ . In the two cases,  $\chi_\pi(\sigma) = \omega$ .

Let  $\gamma \in D$ , where  $\gamma$  is primary. Then  $\gamma = \pm \gamma_1^{n_1} \gamma_2^{n_2} \cdots \gamma_p^{n_p}$ , where the  $\gamma_i$  are distinct primary primes. Write  $n_i = 3q_i + r_i$ ,  $r_i \in \{0, 1, 2\}$ . Then grouping in  $\gamma'$  the  $\gamma^{r_i}$  such that  $r_i \neq 0$ , we can write  $\gamma = \delta^3 \gamma'$ ,  $\gamma' = \gamma_1^{r_1} \gamma_2^{r_2} \cdots \gamma_l^{r_l}$ ,  $r_i \in \{1, 2\}$ ,  $\delta = \pm \gamma_1^{q_1} \cdots \gamma_p^{q_p} \in D$  ( $-1$  is a cube). Since by hypothesis  $\gamma$  is not a cube,  $l \geq 1$ . Moreover the equation  $x^3 \equiv \gamma \pmod{\pi}$  is solvable iff  $x^3 \equiv \gamma' \pmod{\pi}$  is solvable. We may then suppose that

$$\gamma = \gamma_1^{r_1} \gamma_2^{r_2} \cdots \gamma_l^{r_l}, 1 \leq r_i \leq 2,$$

without cubic factors.

Note that the  $\gamma_i$  are not associate to  $\lambda = 1 - \omega$  (see Ex. 9.17).

Let  $A = \{\lambda_1, \lambda_2, \dots, \lambda_k\}$  a set (possibly empty) of distinct primary primes  $\lambda_i$  (therefore they are not associate), and not associate neither to  $\gamma_i$ ,  $1 \leq i \leq l$ , nor to  $\lambda = 1 - \omega$ .

We will show that we can find a primary prime  $\lambda_{k+1}$  distinct of the  $\lambda_i$  with the same properties and such that the equation  $x^3 \equiv \lambda \pmod{\lambda_{k+1}}$  is not solvable. This will prove the existence of infinitely many primes  $\pi$  such that the equation  $x^3 \equiv \lambda \pmod{\pi}$  is not solvable.

Using the initial note, let  $\sigma \in D$  such that  $\chi_{\gamma_l}(\sigma) = \omega$ . As  $D$  is a principal ideal domain, the Chinese Remainder Theorem is valid. Since  $3 = \lambda \bar{\lambda} = -\omega^2 \lambda^2$  is relatively prime to  $\gamma_i, \lambda_i$ , there exists  $\beta \in D$  such that

$$\begin{aligned} \beta &\equiv 2 \pmod{3}, \\ \beta &\equiv 1 \pmod{\lambda_i} & (1 \leq i \leq k), \\ \beta &\equiv 1 \pmod{\gamma_i} & (1 \leq i \leq l-1), \\ \beta &\equiv \sigma \pmod{\gamma_l}. \end{aligned}$$

The first equation show that  $\beta$  is primary, so  $\beta = (-1)^{m-1} \beta_1 \cdots \beta_m$ , where the  $\beta_i$  are primary primes.

By Exercise 9.20,

$$\chi_\beta(\gamma) = \chi_\beta(\gamma_1)^{r_1} \cdots \chi_\beta(\gamma_l)^{r_l} = \chi_{\gamma_1}(\beta)^{r_1} \cdots \chi_{\gamma_l}(\beta)^{r_l}.$$

As  $\chi_{\gamma_i}(1) = 1$  ( $1 \leq i \leq l-1$ ), and  $\chi_{\gamma_l}(\beta) = \chi_{\gamma_l}(\sigma) = \omega$ , we obtain  $\chi_\beta(\gamma) = \omega^{r_l} \neq 1$ , since  $r_l = 1$  or  $r_l = 2$ .

By Exercise 9.18,  $\chi_\rho(\alpha)\chi_\gamma(\alpha) = \chi_{-\rho\gamma}(\alpha)$ , with primary  $\rho, \gamma$ , so by induction, as  $\beta = (-1)^{m-1}\beta_1 \cdots \beta_m$ ,

$$\chi_\beta(\gamma) = \chi_{\beta_1}(\gamma) \cdots \chi_{\beta_m}(\gamma) \neq 1.$$

Thus there exists a subscript  $j$  such that  $\chi_{\beta_j}(\gamma) \neq 1$ .

We can then take  $\lambda_{k+1} = \beta_j$ . Indeed, since  $\beta \equiv 1 [\lambda_i]$  and  $\beta \not\equiv 0 [\gamma_i]$ ,  $\beta_j$  is distinct of the  $\lambda_i$  and  $\gamma_i$ , and  $\beta_j$  is not associate to  $\lambda$  since  $\beta \equiv 2 \pmod{3}$ .

As  $\chi_{\lambda_{k+1}}(\gamma) \neq 1$ , the equation  $x^3 \equiv \gamma [\lambda_{k+1}]$  is not solvable, so  $\lambda_{k+1}$  is convenient.

Conclusion : if  $\gamma \in D$  is primary and is not a cube in  $D$ , there exist infinitely many primes  $\pi \in D$  such that the equation  $x^3 \equiv \gamma [\pi]$  is not solvable.

- b) We show that  $x^3 \equiv \omega [\pi]$  has no solution for infinitely many primes  $\pi$ .

To initialize the induction, we display such a prime  $\pi$ , namely  $\pi = 2 + 3\omega$ . Indeed,  $N(\pi) = 4 + 9 - 6 = 7$ , 7 is a rational prime, so  $\pi$  is a primary prime in  $D$ , of the form  $\pi = 3m - 1 + 3n\omega$ , with  $n = m = 1$ , so  $\chi_\pi(\omega) = \omega^{m+n} = \omega^2 \neq 1$  : the equation  $x^3 \equiv \omega [\pi]$  is not solvable. Moreover  $\pi$  is not associate to  $\lambda = 1 - \omega$ .

Suppose now the existence of a set  $A = \{\lambda_1, \lambda_2, \dots, \lambda_l\}, l \geq 1$ , of distinct primary primes  $\lambda_i$ , not associate to  $\lambda$  and such the equation  $x^3 \equiv \omega [\lambda_i]$  is not solvable for each  $i$ ,  $1 \leq i \leq l$ . We will show that we can add a prime  $\lambda_{l+1}$  to the set  $A$  with the same properties.

Let

$$\beta = 3(-1)^{l-1}\lambda_1 \cdots \lambda_l - 1.$$

$(-1)^{l-1}\lambda_1 \cdots \lambda_l$  is primary, so  $(-1)^{l-1}\lambda_1 \cdots \lambda_l = 3m - 1 + 3n\omega$ ,  $m, n \in \mathbb{Z}$ .

$\beta = 3(3m - 1 + 3n\omega) - 1 = 3(3m - 1) - 1 + 9n\omega = 3M - 1 + 3N\omega$ , where  $M = 3m - 1, N = 3n$ . By Exercise 9.19,

$$\chi_\beta(\omega) = \omega^{M+N} = \omega^{3m-1+3n} = \omega^2 \neq 1.$$

As  $\beta = \pm\beta_1 \cdots \beta_m$ , where the  $\beta_i$  are primary primes,  $\chi_\beta(\omega) = \chi_{\beta_1}(\omega) \cdots \chi_{\beta_m}(\omega) \neq 1$ , so there exists a subscript  $i$  such that  $\chi_{\beta_i}(\omega) \neq 1$ .

Since  $\beta = 3(-1)^{l-1}\lambda_1 \cdots \lambda_l - 1$ ,  $\beta_i$  is associate neither to  $\lambda_i$  nor to  $\lambda$ . Moreover  $\chi_{\beta_i}(\omega) \neq 1$ , thus the equation  $x^3 \equiv \omega [\beta_i]$  is not solvable:  $\lambda_{l+1} = \beta_i$  is convenient.

Conclusion: the equation  $x^3 \equiv \omega [\pi]$  is not solvable for infinitely many primes  $\pi$ .

- c) We show that  $x^3 \equiv \lambda [\pi]$  has no solution for infinitely many primes  $\pi$ .

To initialize the induction, we display such a prime  $\pi$ , namely  $\pi = -4 + 3\omega$ . Indeed,  $N(\pi) = 16 + 9 + 12 = 37$ , 37 is a rational prime, so  $\pi$  is a primary prime in  $D$ , of the form  $\pi = 3m - 1 + 3n\omega$ , with  $m = -1, n = 1$ , so  $\chi_\pi(\lambda) = \omega^{2m} = \omega \neq 1$  : the equation  $x^3 \equiv \lambda [\pi]$  is not solvable.

Suppose now the existence of a set  $A = \{\lambda_1, \lambda_2, \dots, \lambda_l\}, l \geq 1$ , of distinct primary primes  $\lambda_i$ , not associate to  $\lambda$  and such the equation  $x^3 \equiv \lambda [\lambda_i]$  is not solvable. We will show that we can add a prime  $\lambda_{l+1}$  to the set  $A$  with the same properties.

Let

$$\beta = 3(-1)^{l-1}\lambda_1 \cdots \lambda_l - 1.$$

$(-1)^{l-1}\lambda_1 \cdots \lambda_l$  is primary, so  $(-1)^{l-1}\lambda_1 \cdots \lambda_l = 3m - 1 + 3n\omega$ ,  $m, n \in \mathbb{Z}$ .

$\beta = 3(3m - 1 + 3n\omega) - 1 = 3(3m - 1) - 1 + 9n\omega = 3M - 1 + 3N\omega$ , where  $M = 3m - 1, N = 3n$ . By Exercise 9.19,

$$\chi_\beta(\lambda) = \omega^{2M} = \omega^{2(3m-1)} = \omega \neq 1.$$

As  $\beta = \pm\beta_1 \cdots \beta_m$ , where the  $\beta_i$  are primary primes,  $\chi_\beta(\omega) = \chi_{\beta_1}(\omega) \cdots \chi_{\beta_m}(\omega) \neq 1$ , so there exists a subscript  $i$  such that  $\chi_{\beta_i}(\lambda) \neq 1$ .

Since  $\beta = 3(-1)^{l-1}\lambda_1 \cdots \lambda_l - 1$ ,  $\beta_i$  is associate neither to  $\lambda_i$  nor to  $\lambda$ . Moreover  $\chi_{\beta_i}(\lambda) \neq 1$ , thus the equation  $x^3 \equiv \lambda [\beta_i]$  is not solvable :  $\lambda_{l+1} = \beta_i$  is convenient.

Conclusion : the equation  $x^3 \equiv \lambda [\pi]$  is not solvable for infinitely many primes  $\pi$ .  $\square$

**Ex. 9.22** (continuation) Show in general that if  $\gamma \in D$  and  $x^3 \equiv \gamma \pmod{\pi}$  is solvable for all but finitely many primary primes  $\pi$ , then  $\gamma$  is a cube in  $D$ .

*Proof.* Let  $\gamma \in D$  and suppose that  $\gamma$  is not a cube in  $D$ . We will show that the equation  $x^3 \equiv \gamma [\pi]$  is not solvable for infinitely primes  $\pi \in D$ .

By Exercise 9.2, we can write

$$\gamma = (-1)^u \omega^v \lambda^w \gamma_1^{n_1} \cdots \gamma_p^{n_p},$$

where the  $\gamma_i$  are distinct primary primes, not associate to  $\lambda$ . Let  $v = 3q + b, w = 3q' + c, n_i = 3q_i + r_i$ , with the remainders  $b, c, r_i$  in  $\{0, 1, 2\}$ . Grouping the factors with null remainders, we obtain  $\gamma = \delta^3 \gamma', \gamma' = \omega^b \lambda^c \gamma_1^{r_1} \cdots \gamma_l^{r_l}$ , with  $b, c, r_i$  in  $\{1, 2\}, \delta \in D, l \geq 0$  ( $-1$  is a cube).

Moreover the equation  $x^3 \equiv \gamma [\pi]$  is solvable iff the equation  $x^3 \equiv \gamma' [\pi]$  is solvable. So we may suppose that

$$\gamma = \omega^b \lambda^c \gamma_1^{r_1} \cdots \gamma_l^{r_l}, \quad b \in \{1, 2\}, c \in \{1, 2\}, r_i \in \{1, 2\},$$

without cubic factors.

- Case 1 :  $l \geq 1$ .

Let  $A = \{\lambda_1, \dots, \lambda_k\}$  a possibly empty set of distinct primary primes  $\lambda_i$ , distinct of the  $\gamma_i$ , not associate to  $\lambda$ , and such that the equation  $x^3 \equiv \gamma [\lambda_i]$  is not solvable. We will show that we can add a prime  $\lambda_{k+1}$  with the same properties.

Suppose that  $l \geq 1$ . We have proved in Ex. 9.21 that there exists  $\sigma \in D$  such that  $\chi_{\gamma_l}(\sigma) = \omega$ . Since  $9, \lambda_i, \gamma_j$  are relatively prime, there exists  $\beta \in D$  such that

$$\begin{aligned} \beta &\equiv -1 [9] \\ \beta &\equiv 1 [\lambda_i], 1 \leq i \leq k \\ \beta &\equiv 1 [\gamma_i], 1 \leq i \leq l-1 \\ \beta &\equiv \sigma [\gamma_l] \end{aligned}$$

$\beta \equiv -1 [9]$ , thus  $\beta \equiv -1 [3]$  :  $\beta$  is primary, of the form  $\beta = 3M - 1 + 3N\omega$ .

$\beta = 3M - 1 + 3N\omega \equiv -1 [9]$ , so  $3M + 3N\omega \equiv 0 [9]$ ,  $M + N\omega \equiv 0 [3]$ , thus  $3 \mid M, 3 \mid N$ .

By Exercise 9.18,

$$\begin{aligned}\chi_\beta(\omega) &= \omega^{M+N} = 1 \\ \chi_\beta(\lambda) &= \omega^{2M} = 1\end{aligned}$$

As  $\beta$  and  $\gamma_i$  are primary,  $\chi_\beta(\gamma_i) = \chi_{\gamma_i}(\beta) = \chi_{\gamma_i}(1) = 1$  ( $1 \leq i \leq l-1$ ).

$$\chi_\beta(\gamma) = \chi_\beta(\omega)^b \chi_\beta(\lambda)^c \chi_\beta(\gamma_1)^{r_1} \cdots \chi_\beta(\gamma_l)^{r_l} = \chi_\beta(\gamma_l)^{r_l} = \chi_{\gamma_l}(\beta)^{r_l} = \chi_{\gamma_l}(\sigma)^{r_l} = \omega^{r_l} \neq 1, \text{ since } r_l \in \{1, 2\}.$$

$\beta = \pm\beta_1 \cdots \beta_m$ , with  $\beta_i$  primary primes, therefore

$$\chi_\beta(\gamma) = (\chi_{\beta_1} \cdots \chi_{\beta_m})(\gamma) \neq 1.$$

Thus there exists a subscript  $i$  such that  $\chi_{\beta_i}(\gamma) \neq 1$ , so  $x^3 \equiv \gamma [\beta_i]$  is not solvable. Moreover  $\beta \equiv 1 [\gamma_i]$ , so  $\beta_i$  is not associate to any  $\gamma_j$ . Similarly,  $\beta_i$  is not associate to any  $\gamma_j$ , and  $\beta \equiv -1 [9]$ , therefore  $\beta_i$  is not associate to  $\lambda$ . So  $\lambda_{k+1} = \beta_i$  is convenient.

There exist infinitely many  $\pi$  such that  $x^3 \equiv \gamma [\pi]$  is not solvable.

- Case 2 :  $l = 0$ , so  $\gamma = \omega^b \lambda^c$ ,  $1 \leq b \leq 2, 1 \leq c \leq 2$ .

$\pi_0 = 2 - 3\omega$  is a primary prime ( $N(\pi_0) = 19$ ).

Let  $A = \{\lambda_1, \dots, \lambda_k\}$  a possibly empty set of distinct primary primes  $\lambda_i \neq \pi_0$  such that the equation  $x^3 \equiv \gamma [\lambda_i]$  is not solvable. We will show that we can add a prime  $\lambda_{k+1}$  with the same properties.

Let  $\beta = 9(-1)^{k-1} \lambda_1 \cdots \lambda_k + 2 - 3\omega$ .

$\beta \equiv 2 [3]$  :  $\beta$  is primary.

Moreover  $(-1)^{k-1} \lambda_1 \cdots \lambda_k$  is primary, so

$$(-1)^{k-1} \lambda_1 \cdots \lambda_k = 3m - 1 + 3n\omega, m \in \mathbb{Z}, n \in \mathbb{Z}.$$

Then

$$\begin{aligned}\beta &= 9(3m - 1 + 3n\omega) + 2 - 3\omega \\ &= 27m - 7 + (27n - 3)\omega \\ &= 3(9m - 2) - 1 + 3(9n - 1)\omega \\ &= 3M - 1 + 3N\omega,\end{aligned}$$

where  $M = 9m - 2, N = 9n - 1$ . Therefore

$$\begin{aligned}\chi_\beta(\omega) &= \omega^{M+N} = \omega^{9m-2+9n-1} = 1 \\ \chi_\beta(\lambda) &= \omega^{2M} = \omega^{2(9m-2)} = \omega^2 \neq 1\end{aligned}$$

$\beta = \pm\beta_1 \cdots \beta_m$ , where the  $\beta_i$  are primary primes.

$\chi_\beta(\gamma) = \chi_\beta(\omega)^b \chi_\beta(\lambda)^c = \omega^{2c} \neq 1$  since  $c = 1$  or  $c = 2$ .

$$\chi_\beta(\gamma) = (\chi_{\beta_1} \cdots \chi_{\beta_m})(\gamma) \neq 1.$$

Thus there exists a subscript  $i$  such that  $\chi_{\beta_i}(\gamma) \neq 1$ , so  $x^3 \equiv \gamma [\beta_i]$  is not solvable.

As  $\beta_i \mid \beta = 9(-1)^{k-1}\lambda_1 \cdots \lambda_k + 2 - 3\omega$ , if  $\beta_i = \lambda_j$  for some subscript  $j$ ,  $\lambda_j \mid \pi_0 = 2 - 3\omega$ , so  $\lambda_j = \pi_0$ , which is a contradiction, thus  $\beta_i \notin A$ . Similarly, if  $\beta_i = \pi_0 = 2 - 3\omega$ , then  $\pi_0 \mid 9\lambda_1 \cdots \lambda_k$ , and  $\pi_0$  is relatively prime to  $\lambda$ , so  $\pi_0 = \lambda_j$  for some subscript  $j$ : this is a contradiction, thus  $\beta_i \neq \pi_0$ .  $\lambda_{k+1} = \beta_i$  is convenient.

So there exist infinitely many  $\pi$  such that  $x^3 \equiv \gamma [\pi]$  is not solvable.

• Conclusion :

if  $\gamma$  is not a cube in  $D$ , there exist infinitely many primes  $\pi$  such that  $x^3 \equiv \gamma [\pi]$  is not solvable.

By contraposition, if the equation  $x^3 \equiv \gamma [\pi]$  is solvable for every prime  $\pi$ , at the exception perhaps of the primes in a finite set, then  $\gamma$  is a cube in  $D$ .

□

**Ex. 9.23** Suppose that  $p \equiv 1 \pmod{3}$ . Use Exercise 5 to show that  $x^3 \equiv 3 \pmod{p}$  is solvable in  $\mathbb{Z}$  iff  $p$  is of the form  $4p = C^2 + 243B^2$ .

*Proof.* Let  $p$  be a rational prime,  $p \equiv 1 \pmod{3}$ , then  $p = \pi\bar{\pi}$ , where  $\pi \in D$  is a primary prime :  $\pi = a + b\omega = 3m - 1 + 3n\omega$ .

- Suppose that there exists  $x \in \mathbb{Z}$  such that  $x^3 \equiv 3 \pmod{p}$ . Then  $x^3 \equiv 3 \pmod{\pi}$ , so  $\chi_\pi(3) = 1$ . By Exercise 9.5,  $\omega^{2n} = \chi_\pi(3) = 1$ , thus  $3 \mid n$ , therefore  $9 \mid b = 3n$ , namely  $b = 9B, B \in \mathbb{Z}$ .

$p = N\pi = a^2 + b^2 - ab, 4p = (2a - b)^2 + 3b^2 = C^2 + 243B^2$ , where  $C = 2a - b, B = b/9$ . So there exists  $C, B \in \mathbb{Z}$  such that  $4p = C^2 + 243B^2$ .

- Conversely, suppose that there exist  $C, B \in \mathbb{Z}$  such that  $4p = C^2 + 243B^2$ .

As  $4p = (2a - b)^2 + 3b^2 = C^2 + 3(9B)^2$ , from the unicity proved in Exercise 8.13, we obtain  $b = \pm 9B$ , so  $9 \mid b = 3n, 3 \mid n$ , and  $\chi_\pi(3) = \omega^{2n} = 1$ .

Thus there exists  $x \in D$  such that  $x^3 \equiv 3 \pmod{\pi}$ . As  $p \equiv 1 \pmod{3}$ ,  $D/\pi D = \{\bar{0}, \dots, \bar{p-1}\}$ , so there exists  $h \in \mathbb{Z}$  such that  $x \equiv h \pmod{\pi}$ , and  $h^3 \equiv 3 \pmod{\pi}$ .

Therefore  $p = N\pi \mid N(h^3 - 3)$ , namely  $p \mid (h^3 - 3)^2$ , where  $p$  is a rational prime, thus  $p \mid h^3 - 3$ : there exists  $x \in \mathbb{Z}$  such that  $x^3 \equiv 3 \pmod{p}$ .

Moreover  $4p = C^2 + 243B^2$  implies  $p \equiv 1 \pmod{3}$ .

$$(p \equiv 1 \pmod{3} \text{ and } \exists x \in \mathbb{Z}, x^3 \equiv 3 \pmod{p}) \iff \exists C \in \mathbb{Z}, \exists B \in \mathbb{Z}, 4p = C^2 + 243B^2.$$

□

**Ex. 9.24** Let  $\pi = a + b\omega$  be a complex primary element of  $D = \mathbb{Z}[\omega]$ . Put  $a = 3m - 1, b = 3n, p = N(\pi)$ .

(a)  $(p - 1)/3 \equiv -2m + n \pmod{3}$ .

(b)  $(a^2 - 1)/3 \equiv m \pmod{3}$ .

(c)  $\chi_\pi(a) = \omega^m$ .

(d)  $\chi_\pi(a + b) = \omega^{2n}\chi_\pi(1 - \omega)$ .



**Lemma.** Let  $a \in \mathbb{Z}$ ,  $a \equiv -1 \pmod{3}$ , and  $b \in \mathbb{Z}$  such that  $a \wedge b = 1$ . Then  $\chi_a(b) = 1$ .

*Proof.* (of Lemma.)

If  $q$  is a rational prime,  $q \equiv 2 \pmod{3}$ , and  $q \wedge b = 1$ , then  $\chi_q(b) = 1$  (Prop. 9.3.4, Corollary).

If  $p$  is a rational prime,  $p \equiv 1 \pmod{3}$  and  $p \wedge b = 1$ , then  $p = \pi \bar{\pi}$ , with  $\pi$  primary prime in  $D$  (and also  $\bar{\pi}$ ), and by definition of  $\chi_p$ ,  $\chi_p(b) = \chi_\pi(b) \chi_{\bar{\pi}}(b)$ .

As  $\chi_{\bar{\pi}}(b) = \chi_{\bar{\pi}}(\bar{b}) = \overline{\chi_\pi(b)}$  (Prop. 9.3.4(b)), then  $\chi_p(b) = \chi_\pi(b) \chi_{\bar{\pi}}(b) = \chi_\pi(b) \overline{\chi_\pi(b)} = 1$ .

$a$  has a decomposition in prime factors of the form :

$$a = \pm q_1 q_2 \cdots q_k p_1 p_2 \cdots p_l = \pm q_1 q_2 \cdots q_k \pi_1 \bar{\pi}_1 \pi_2 \bar{\pi}_2 \cdots \pi_l \bar{\pi}_l,$$

where  $q_i \equiv -1, p_j \equiv 1 \pmod{3}$ , and the  $\pi_k$  are primary primes (since all these elements are primary, the symbol  $\pm$  is  $(-1)^{k-1}$ ). Thus, by definition of  $\chi_a$ ,

$$\chi_a(b) = \chi_{q_1}(b) \cdots \chi_{q_k}(b) \chi_{\pi_1}(b) \chi_{\bar{\pi}_1}(b) \cdots \chi_{\pi_l}(b) \chi_{\bar{\pi}_l}(b) = 1.$$

The result remains true if  $a = -1$  : then, by definition,  $\chi_a(b) = 1$ .

□

*Proof.* (of Ex 9.24.) By hypothesis,  $\pi$  is a primary element, so  $\pi = 3m - 1 + 3n\pi$ ,  $m, n \in \mathbb{Z}$ . We don't suppose in this proof that  $\pi$  is a prime element, so  $p = N(\pi)$  is not necessarily prime.

(a)  $p - 1 = (3m - 1)^2 + (3n)^2 - 3n(3m - 1) - 1 \equiv -6m + 3n \pmod{9}$ , thus

$$\frac{p-1}{3} \equiv -2m + n \pmod{3}.$$

(b)  $a^2 - 1 = (3m - 1)^2 - 1 \equiv -6m \pmod{9}$ , thus

$$\frac{a^2 - 1}{3} \equiv m \pmod{3}.$$

(c) As  $\pi, a$  are primary, by Exercise 9.20,  $\chi_\pi(a) = \chi_a(\pi)$ .

Since  $\pi \equiv b\omega \pmod{a}$ ,  $\chi_a(\pi) = \chi_a(b) \chi_a(\omega)$ .

By Exercise 9.18, as  $a = 3m - 1$ ,  $\chi_a(\omega) = \omega^{M+N}$ , where  $M = m, N = 0$ , so

$$\chi_a(\omega) = \omega^m.$$

Here  $a$  is relatively prime to  $b$  in  $\mathbb{Z}$  : if a rational prime  $r$  divides  $a, b$ , then  $r \mid \pi$  in  $D$ , thus  $r \mid \bar{\pi}$ , so  $r^2 \mid \pi \bar{\pi} = p$  in  $D$ , thus  $r^2 \mid p$  in  $\mathbb{Z}$ , which is absurd. The Lemma gives then  $\chi_a(b) = 1$ .

We conclude that  $\chi_a(b) = 1, \chi_a(\omega) = \omega^m$ , so  $\chi_\pi(a) = \chi_a(\pi) = \chi_a(b) \chi_a(\omega) = \omega^m$ .

$$\chi_\pi(a) = \omega^m.$$

(d)

$$a + b = [(a + b)\omega]\omega^{-1},$$

and

$$(a + b)\omega = (a + b\omega) + a\omega - a \equiv a(\omega - 1) \pmod{\pi},$$

thus

$$a + b \equiv -a(1 - \omega)\omega^{-1} \pmod{\pi},$$

$$\chi_{\pi}(a + b) = \chi_{\pi}(1 - \omega)\chi_{\pi}(a)\chi_{\pi}(\omega)^{-1},$$

$\chi_{\pi}(a) = \omega^m$  by (c), and  $\chi_{\pi}(\omega) = \omega^{m+n}$  (as in Ex. 9.3), thus

$$\chi_{\pi}(a + b) = \omega^{2n}\chi_{\pi}(1 - \omega).$$

□

**Ex. 9.25** Show that  $\chi_{a+b}(\pi)$  may be computed as follows.

(a)  $\chi_{a+b}(\pi) = \chi_{a+b}(1 - \omega).$

(b)  $\chi_{a+b}(\pi) = \omega^{2(m+n)}.$

*Proof.* (a)  $\pi = a + b\omega$  and  $a \equiv -b \pmod{a + b}$ , thus  $\pi \equiv -b(1 - \omega) \pmod{a + b}$ . So

$$\chi_{a+b}(\pi) = \chi_{a+b}(b)\chi_{a+b}(1 - \omega).$$

Since  $a \wedge b = 1$ ,  $(a + b) \wedge b = 1$  : as in Ex. 9.24,  $\chi_{a+b}(b) = 1$ . So

$$\chi_{a+b}(\pi) = \chi_{a+b}(1 - \omega).$$

(b) Since the character  $\chi_{a+b}$  has order 3,

$$\begin{aligned} \chi_{a+b}(1 - \omega) &= (\chi_{a+b}((1 - \omega)^2))^2 \\ &= (\chi_{a+b}(-3\omega))^2 \\ &= [\chi_{a+b}(3)\chi_{a+b}(\omega)]^2 \end{aligned}$$

$$\chi_{a+b}(3) = 1 \text{ because } (a + b) \wedge 3 = (3(m + n) - 1) \wedge 3 = 1.$$

$$\chi_{a+b}(\omega) = \omega^{m+n} \text{ (Ex. 9.19).}$$

Conclusion :

$$\chi_{a+b}(1 - \omega) = \omega^{2(m+n)}.$$

□

**Ex. 9.26** Combine the previous two exercises to conclude that  $\chi_{\pi}(1 - \omega) = \omega^{2m}$ .

*Proof.* Since  $\pi$  and  $a + b$  are primary elements of  $D$ , by Exercise 9.20,

$$\chi_{\pi}(a + b) = \chi_{a+b}(\pi).$$

By Exercises 9.24 and 9.25,

$$\chi_{\pi}(a + b) = \omega^{2n}\chi_{\pi}(1 - \omega)$$

$$\chi_{a+b}(\pi) = \omega^{2(m+n)}$$

Thus  $\omega^{2n}\chi_{\pi}(1 - \omega) = \omega^{2(m+n)}$ . Consequently

$$\chi_{\pi}(1 - \omega) = \omega^{2m}.$$

□

**Ex. 9.27** Let  $\pi = a + bi$  be a primary irreducible in  $\mathbb{Z}[i]$ ,  $b \neq 0$ . Show

$$(a) \ a \equiv (-1)^{(p-1)/4} \pmod{4}, \ p = N(\pi).$$

$$(b) \ b \equiv (-1)^{(p-1)/4} - 1 \pmod{4}.$$

(Wrong sentence for (b) in the edition 1990.)

*Proof.* Let  $\pi = a + bi$  be a primary prime in  $\mathbb{Z}[i]$ ,  $b \neq 0$ , such that  $p = N(\pi)$ . Then

$$p = \pi \bar{\pi} = a^2 + b^2 \equiv 1 \pmod{4}.$$

By Lemma 6, Section 7,  $a$  is odd,  $b$  even, and

$$(a \equiv 1 \pmod{4}, b \equiv 0 \pmod{4}) \text{ or } (a \equiv 3 \pmod{4}, b \equiv 2 \pmod{4}).$$

- (a) • Case 1:  $a \equiv 1 \pmod{4}, b \equiv 0 \pmod{4}$ . Then  $a = 4A + 1, b = 4B$ ,  $A, B \in \mathbb{Z}$ , so  $(a^2 + b^2 - 1)/4 = 4A^2 + 4B^2 + 2A$  is even :  
 $(-1)^{(p-1)/4} = (-1)^{(a^2+b^2-1)/4} = 1$ , and  $a \equiv 1 \pmod{4}$ , thus  $a \equiv (-1)^{(p-1)/4} \pmod{4}$ .  
 • Case 2:  $a \equiv 3 \pmod{4}, b \equiv 2 \pmod{4}$ .  
 $a = 4A + 3, b = 4B + 2, a^2 + b^2 - 1 = 16A^2 + 24A + 9 + 16B^2 + 16B + 4 - 1 \equiv 4 \pmod{8}$ ,  
 so  $(a^2 + b^2 - 1)/4 \equiv 1 \pmod{2}$ ,  $(-1)^{(p-1)/4} = (-1)^{(a^2+b^2-1)/4} = -1$ , and  $a \equiv -1 \pmod{4}$ ,  
 thus  $a \equiv (-1)^{(p-1)/4} \pmod{4}$ .

In both cases,

$$a \equiv (-1)^{(p-1)/4} \pmod{4}.$$

- (b) In every case,  $b \equiv a - 1 \pmod{4}$ , thus

$$b \equiv (-1)^{(p-1)/4} - 1 \pmod{4}.$$

In other words, for all primary primes  $\pi = a + bi$  such that  $N(\pi) = p$ ,

$$\begin{aligned} p \equiv 1 \pmod{8} &\iff \pi \equiv 1 \pmod{4}, \\ p \equiv 5 \pmod{8} &\iff \pi \equiv 3 + 2i \pmod{4}. \end{aligned}$$

□

**Ex. 9.28** The notation being as in Exercise 27 show  $\chi_\pi(\bar{\pi}) = \chi_\pi(2)\chi_\pi(a)$ .

*Proof.*  $\pi = a + bi, \bar{\pi} = a - bi = 2a - \pi \equiv 2a \pmod{\pi}$ , thus, by Proposition 9.8.3 (e) :

$$\chi_\pi(\bar{\pi}) = \chi_\pi(2a) = \chi_\pi(2)\chi_\pi(a).$$

□

**Ex. 9.29** By Exercise 9.27,  $a(-1)^{(p-1)/4}$  is primary. Use biquadratic reciprocity to show  $\chi_\pi(a(-1)^{(p-1)/4}) = (-1)^{(a^2-1)/8}$ .

*Proof.*  $a \equiv (-1)^{(p-1)/4} [4]$  (Ex. 9.27(a)),  $a(-1)^{(p-1)/4} \equiv 1 [4]$ , thus  $a(-1)^{(p-1)/4}$  is primary (if  $a \neq \pm 1$ ).

If  $a = \pm 1$  is a unit,  $a(-1)^{(p-1)/4} = 1$  and  $\chi_\pi(a(-1)^{(p-1)/4}) = 1 = (-1)^{(a^2-1)/8}$ , so we can suppose that  $a$  is not a unit.

As  $a(-1)^{(p-1)/4} \equiv 1 \pmod{4}$ , the Law of Biquadratic Reciprocity (Prop. 9.9.8) gives

$$\begin{aligned}\chi_\pi(a(-1)^{(p-1)/4}) &= \chi_{a(-1)^{(p-1)/4}}(\pi) \\ &= \chi_a(\pi) \quad (\text{Prop. 9.8.3(f)}) \\ &= \chi_a(a + bi) \\ &= \chi_a(bi) \\ &= \chi_a(b)\chi_a(i).\end{aligned}$$

As  $a \wedge b = 1$  (since  $p = a^2 + b^2$ ),  $\chi_a(b) = 1$  (Prop. 9.8.5, with  $a \neq 1$ ), so

$$\chi_\pi(a(-1)^{(p-1)/4}) = \chi_a(i).$$

If  $a \equiv 1 [4]$ , Proposition 9.8.6 gives  $\chi_a(i) = (-1)^{(a-1)/4}$ . Write  $a = 4A + 1$ ,  $A \in \mathbb{Z}$ . Then

$$(-1)^{(a^2-1)/8} = (-1)^{2A^2+A} = (-1)^A = (-1)^{(a-1)/4} = \chi_a(i).$$

If  $a \equiv -1 [4]$ , then  $\chi_a(i) = \chi_{-a}(i) = (-1)^{(-a-1)/4}$  by the same proposition. Write  $a = 4A - 1$ ,  $A \in \mathbb{Z}$ . Then

$$(-1)^{(a^2-1)/8} = (-1)^{2A^2-A} = (-1)^{-A} = (-1)^{(-a-1)/4} = \chi_a(i).$$

So, for each odd  $a$ ,  $a \neq \pm 1$ ,

$$\chi_a(i) = i^{(a^2-1)/8}.$$

Conclusion : if  $\pi = a + bi$  is a primary irreducible such that  $N(\pi) = p$ , then

$$\chi_\pi(a(-1)^{(p-1)/4}) = (-1)^{(a^2-1)/8}.$$

□

**Ex. 9.30** Use the preceding two exercises to show  $\chi_\pi(\bar{\pi}) = \chi_\pi(2)(-1)^{(a^2-1)/8}$ .

*Proof.* By Exercises 9.28, 9.29, and  $\chi_\pi(-1) = (-1)^{(a-1)/2}$  (Prop. 9.8.3(d)),

$$\begin{aligned}\chi_\pi(\bar{\pi}) &= \chi_\pi(2)\chi_\pi(a) \\ &= \chi_\pi(2)\chi_\pi(a(-1)^{(p-1)/4})(\chi_\pi(-1))^{(p-1)/4} \\ &= \chi_\pi(2)(-1)^{(a^2-1)/8}((-1)^{(a-1)/2})^{(p-1)/4} \\ &= \chi_\pi(-2)(-1)^{(a^2-1)/8}((-1)^{(a-1)/2})^{(p+3)/4} \\ &= \chi_\pi(-2)(-1)^{(a^2-1)/8}(-1)^{((a-1)/2)((p+3)/4)}.\end{aligned}$$

If  $a \equiv 1 \pmod{4}$ , then  $(-1)^{(a-1)/2} = 1$ .

If  $a \equiv 3 \pmod{4}$ , then  $b \equiv 2 [4]$  :

$$a = 4A + 3, b = 4B + 2, p + 3 = a^2 + b^2 + 3 = (4A + 3)^2 + (4B + 2)^2 + 3 \equiv 0 [8],$$

so  $(p+3)/4 \equiv 0 \pmod{2}$ .

In both cases  $(-1)^{((a-1)/2)((p+3)/4)} = 1$ , and so

$$\chi_\pi(\bar{\pi}) = \chi_\pi(-2)(-1)^{(a^2-1)/8}.$$

□

**Ex. 9.31** Let  $p$  be prime,  $p \equiv 1 \pmod{4}$ . Show that  $p = a^2 + b^2$  where  $a$  and  $b$  are uniquely determined by the conditions  $a \equiv 1 \pmod{4}$ ,  $b \equiv -((p-1)/2)!a \pmod{p}$ .

*Proof.* Recall the following lemma :

**Lemma :**

Let  $p$  be prime,  $p \equiv 1 \pmod{4}$ , then  $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p}$ .

By Wilson's theorem (Prop. 4.1.1, Corollary),  $(p-1)! \equiv -1 \pmod{p}$ .

$$\begin{aligned} -1 &\equiv (p-1)! = 1.2.\dots \cdot \left(\frac{p-1}{2}\right) \left(\frac{p+1}{2}\right) \dots (p-2)(p-1) \\ &\equiv 1.2.\dots \frac{p-1}{2} \left[-\left(\frac{p-1}{2}\right)\right] \dots (-2)(-1) \\ &\equiv (-1)^{(p-1)/2} \left[\left(\frac{p-1}{2}\right)!\right]^2 \\ &\equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}, \end{aligned}$$

since  $p \equiv 1 \pmod{4}$ .

- We show that there exists a pair  $a, b \in \mathbb{Z}$  which verifies the sentence.

By lemma 5 section 7, as  $p \equiv 1 \pmod{4}$ , there exists an irreducible  $\pi$  such that  $N(\pi) = p$ , and we can choose  $\pi$  such that  $\pi = A + Bi$  is primary (lemma 7 section 7), so  $A$  is odd.

If  $A \equiv 1 \pmod{4}$ , we take  $a = A$ , and if  $A \equiv 3 \pmod{4}$ , we take  $a = -A$  : then  $a \equiv 1 \pmod{4}$ .

Let  $u = \left(\frac{p-1}{2}\right)!$ . Then  $0 \equiv p = A^2 + B^2 \pmod{p}$ ,  $B^2 \equiv -A^2 \equiv (uA)^2 \pmod{p}$ .

$p \mid (B - uA)(B + uA)$ , thus  $B \equiv \pm uA \pmod{p}$ .

Since  $a = \pm A$ ,  $B \equiv \pm ua \pmod{p}$ .

If  $B \equiv -ua \pmod{p}$ , we take  $b = B$ , if not  $b = -B$ .

Then  $a, b$  are such that  $p = a^2 + b^2$ ,  $a \equiv 1 \pmod{4}$ ,  $b \equiv -((p-1)/2)!a \pmod{p}$ .

- Unicity of the pair  $(a, b)$  such that

$$p = a^2 + b^2, a \equiv 1 \pmod{4}, b \equiv -((p-1)/2)!a \pmod{p}.$$

Suppose that  $c, d$  are such that  $p = c^2 + d^2$ ,  $c \equiv 1 \pmod{4}$ ,  $d \equiv -((p-1)/2)!c \pmod{p}$ .

Let  $\pi = a + ib, \lambda = c + id$ . As  $p = N\pi = N\lambda$  is a rational prime,  $\pi$  and  $\lambda$  are primes in  $D$ , and  $p = \pi\bar{\pi} = \lambda\bar{\lambda}$ , thus  $\lambda$  is associate to  $\pi$  or  $\bar{\pi}$  :

$$\lambda \in \{\pi, -\pi, i\pi, -i\pi, \bar{\pi}, -\bar{\pi}, i\bar{\pi}, -i\bar{\pi}\}.$$

As  $a, c$  are odd, and  $b, d$  even, it remains only the possibilities  $\lambda = \pm\pi, \lambda = \pm\bar{\pi}$ , thus  $c = \pm a$ . Moreover  $a \equiv c \equiv 1 \pmod{4}$ , thus  $a = c$ , and  $d \equiv -((p-1)/2)!c \equiv -((p-1)/2)!a \equiv b \pmod{p}$ .

$p = a^2 + b^2 = a^2 + d^2$ , so  $d = \pm b$ , and  $d \equiv b \pmod{p}$ .

If  $d = -b$ , then  $p \mid 2b$ , thus  $p \mid b$ , and also  $p \mid a$ , so  $p^2 \mid a^2 + b^2 = p$ : this is impossible. So  $a = b, c = d$ . Unicity is proved.

Conclusion : if  $p \equiv 1 \pmod{4}$ , there exists an unique pair  $a, b$  such that

$$p = a^2 + b^2, a \equiv 1 \pmod{4}, b \equiv -((p-1)/2)!a \pmod{p}.$$

□

**Ex. 9.32** Let  $p$  be a prime,  $p \equiv 1 \pmod{4}$  and write  $p = \pi\bar{\pi}, \pi \in \mathbb{Z}[i]$ . Show  $\chi_p(1+i) = i^{(p-1)/4}$ .

*Proof.*

$$\begin{aligned} \chi_p(1+i) &= \chi_\pi(1+i)\chi_{\bar{\pi}}(1+i) \\ &= \chi_\pi(1+i)\overline{\chi_\pi(1-i)} \quad (\text{Prop. 9.8.3(c)}) \\ &= \frac{\chi_\pi(1+i)}{\chi_\pi(1-i)} = \chi_\pi(i) \quad (\text{since } (1-i)i = 1+i) \\ &= i^{\frac{p-1}{4}}. \end{aligned}$$

The last equality is a consequence of the definition of  $\chi_\pi : \chi_\pi(i) \equiv i^{\frac{p-1}{4}} \pmod{\pi}$ , and the classes of  $1, i, i^2, i^3$  modulo  $\pi$  are distinct. □

**Ex. 9.33** Let  $q$  be a positive prime,  $q \equiv 3 \pmod{4}$ . Show  $\chi_q(1+i) = i^{(q+1)/4}$ . [Hint :  $(1+i)^{q-1} \equiv -i \pmod{q}$ .]

The sentence is false and must be replaced by

$$\chi_q(1+i) = (-i)^{(q+1)/4} = i^{-(q+1)/4}.$$

We verify this on the example  $q = 11$  :

$$\begin{aligned} \chi_q(1+i) &\equiv (1+i)^{(q^2-1)/4} \\ &\equiv (1+i)^{30} \\ &\equiv -2^{15}i \equiv -32i \equiv i \pmod{11}, \end{aligned}$$

so  $\chi_{11}(1+i) = i$ , and  $i^{(-q-1)/4} = i^{-3} = i$  (but  $i^{(q+1)/4} = -i$ ).

*Proof.* Write  $q = 4k + 3, k \in \mathbb{N}$ .

As  $(1+i)^2 = 2i$ ,  $(1+i)^{q-1} = (2i)^{(q-1)/2}$ .

$2^{(q-1)/2} \equiv \left(\frac{2}{q}\right) [q]$  et  $\left(\frac{2}{q}\right) = (-1)^{(q^2-1)/8} = (-1)^{2k^2+3k+1} = (-1)^{k+1}$

$i^{(q-1)/2} = i^{2k+1} = (-1)^k i$ .

So

$$(1+i)^{q-1} \equiv -i [q].$$

$N(q) = q^2$ , so  $\chi_q(1+i) \equiv (1+i)^{(q^2-1)/4} = [(1+i)^{q-1}]^{(q+1)/4} \equiv (-i)^{(q+1)/4} [q] :$

$$\chi_q(1+i) = (-i)^{(q+1)/4} = i^{(-q-1)/4}.$$

□

**Ex. 9.34** Let  $\pi = a + bi$  be a primary irreducible,  $(a, b) = 1$ . Show

(a) if  $\pi \equiv 1 \pmod{4}$ , then  $\chi_\pi(a) = i^{(a-1)/2}$ .

(b) if  $\pi \equiv 3 + 2i \pmod{4}$ , then  $\chi_\pi(a) = -i^{(-a-1)/2}$ .

*Proof.* Let  $\pi = a + bi$  be a primary irreducible, with  $a \wedge b = 1$ , so  $b \neq 0$ . We can apply the result of Exercise 9.29:

$$\chi_\pi(a(-1)^{(p-1)/4}) = (-1)^{(a^2-1)/8}.$$

(a) Suppose that  $\pi \equiv 1 [4]$ .

Then  $a \equiv 1 [4], b \equiv 0 [4], a = 4A + 1, b = 4B, A, B \in \mathbb{Z}$ .

As  $\chi_\pi(-1) = (-1)^{(a-1)/2}$ ,

$$\chi_\pi(a) = (-1)^{\frac{a-1}{2} \frac{p-1}{4}} (-1)^{\frac{a^2-1}{8}},$$

where

$$p = N\pi = a^2 + b^2, (-1)^{(p-1)/4} = (-1)^{\frac{a^2-1}{4} + \frac{b^2}{4}} = (-1)^{4A^2+2A+4B^2} = 1,$$

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

$$\chi_\pi(a) = (-1)^{(a^2-1)/8} = (-1)^{2A^2+A} = (-1)^A = (-1)^{(a-1)/4} = i^{(a-1)/2}.$$

Conclusion: if  $\pi \equiv 1 [4]$ ,  $\chi_\pi(a) = i^{(a-1)/2}$ .

(b) Suppose that  $\pi \equiv 3 + 2i [4]$ .

Then  $a \equiv 3 [4], b \equiv 2 [4], a = 4A + 3, b = 4B + 2, A, B \in \mathbb{Z}$ . As in (a),

$$\chi_\pi(a) = (-1)^{\frac{a-1}{2} \frac{p-1}{4}} (-1)^{\frac{a^2-1}{8}},$$

where  $a^2 + b^2 - 1 = 16A^2 + 24A + 16B^2 + 16B + 12 \equiv 4 [8]$ , so  $\frac{a^2+b^2-1}{4} \equiv 1 [2]$ ,

thus  $(-1)^{(p-1)/4} = (-1)^{(a^2+b^2-1)/4} = -1$ .

$$(-1)^{\frac{a-1}{2} \frac{p-1}{4}} = (-1)^{\frac{a-1}{2}} = (-1)^{2A+1} = -1,$$

$$\frac{a^2-1}{8} = 2A^2 + 3A + 1, (-1)^{(a^2-1)/8} = (-1)^{3A+1} = (-1)^{A+1} = (-1)^{(a+1)/4},$$

$$\chi_\pi(a) = -(-1)^{(a+1)/4} = -i^{(a+1)/2}.$$

Moreover

$$\frac{a+1}{2} \equiv \frac{-a-1}{2} \pmod{4} \iff a+1 \equiv -a-1 \pmod{8} \iff 2a \equiv -2 \pmod{8} \iff a \equiv 3 \pmod{4},$$

thus  $i^{(a+1)/2} = i^{(-a-1)/2}$ .

Conclusion : if  $\pi \equiv 3 + 2i \pmod{4}$ ,  $\chi_\pi(a) = -i^{(-a-1)/2}$ .

□

**Ex. 9.35** If  $\pi = a + bi$  is as in Exercise 9.34 show  $\chi_\pi(a)\chi_\pi(1+i) = i^{(3(a+b-1))/4}$ . [Hint:  $a(1+i) = a+b+i(a+bi)$ . Generalize Exercises 32 and 33 to any integer  $\equiv 1 \pmod{4}$  and use Proposition 9.9.8. Note  $a+b \equiv 1 \pmod{4}$ .]

*Proof.* We give a generalization of Exercises 9.32 and 9.33 : if  $n \equiv 1 \pmod{4}$ ,  $n \neq 1$ , then  $\chi_n(1+i) = i^{(n-1)/4}$ .

By Exercises 9.32 and 9.33, we know that if  $p \equiv 1 \pmod{4}$  is a rational prime, then

$$\chi_p(1+i) = i^{(p-1)/4},$$

and if  $q \equiv 3 \pmod{4}$ , in other words  $-q \equiv 1 \pmod{4}$ , where  $q$  is a rational prime, then

$$\chi_{-q}(1+i) = \chi_q(1+i) = i^{(-q-1)/4}.$$

Let  $n \in \mathbb{Z}$ ,  $n \equiv 1 \pmod{4}$ ,  $n \neq 1$ .

If  $n > 0$ ,  $n = q_1 q_2 \cdots q_k p_1 p_2 \cdots p_l$ , where  $q_i \equiv -1 \pmod{4}$ ,  $p_i \equiv 1 \pmod{4}$ , thus  $k$  is odd.

If  $n < 0$ ,  $n = -q_1 q_2 \cdots q_k p_1 p_2 \cdots p_l$ , with  $k$  odd. In both cases,

$$n = (-q_1)(-q_2) \cdots (-q_k)p_1 p_2 \cdots p_l,$$

so we can write

$$n = s_1 s_2 \cdots s_N, \quad \text{where } s_i = -q_i, 1 \leq i \leq k, s_i = p_{i-k}, k+1 \leq i \leq k+l = N,$$

where  $s_i \equiv 1 \pmod{4}$ ,  $1 \leq i \leq N$ .

$$\begin{aligned} \chi_n(1+i) &= \chi_{-q_1}(1+i) \cdots \chi_{-q_k}(1+i) \chi_{p_1}(1+i) \cdots \chi_{p_l}(1+i) \\ &= i^{(-q_1-1)/4} \cdots i^{(-q_k-1)/4} i^{(p_1-1)/4} \cdots i^{(p_l-1)/4} \\ &= i^{(s_1-1)/4} \cdots i^{(s_N-1)/4} \\ &= i^{\sum_{i=1}^N \frac{s_i-1}{4}} \\ &= i^{(n-1)/4}, \end{aligned}$$

the last equality resulting of Exercise 9.44.

Conclusion : if  $n \in \mathbb{Z}$ ,  $n \equiv 1 \pmod{4}$ ,  $n \neq 1$ , then  $\chi_n(1+i) = i^{(n-1)/4}$ .

Let  $\pi = a + bi$ ,  $a \wedge b = 1$  a primary irreducible. As  $a(1+i) = a+b+i(a+bi)$ ,  $a(1+i) \equiv a+b \pmod{\pi}$ , so

$$\chi_\pi(a)\chi_\pi(1+i) = \chi_\pi(a+b).$$



As  $\pi = a + bi$  is primary,  $a + b \equiv 1 \pmod{4}$ .

If  $a + b = 1$ , then  $\chi_\pi(a)\chi_\pi(1+i) = \chi_\pi(a+b) = 1 = i^{3(a+b-1)/4}$ . If not, the Law of Biquadratic Reciprocity (Proposition 9.9.8) gives

$$\chi_\pi(a+b) = \chi_{a+b}(\pi).$$

Now  $b \equiv -a \pmod{a+b}$ , so  $a + bi \equiv a(1-i) \equiv -ia(1+i) \pmod{a+b}$ . Therefore

$$\chi_{a+b}(\pi) = \chi_{a+b}(-1)\chi_{a+b}(a)\chi_{a+b}(i)\chi_{a+b}(1+i).$$

Since  $n \equiv 1 \pmod{4}$ ,  $\chi_n(i) = (-1)^{(n-1)/4}$  (Prop. 9.8.6), thus

$$\chi_n(-1) = \chi_n(i^2) = (-1)^{\frac{n-1}{2}} = 1.$$

Consequently, since  $a + b \equiv 1 \pmod{4}$ ,  $\chi_{a+b}(-1) = 1$ .

As  $a \wedge b = 1$ ,  $(a+b) \wedge a = 1$ , thus  $\chi_{a+b}(a) = 1$  (Prop 9.8.5).

$a + b \equiv 1 \pmod{4}$ , thus  $\chi_{a+b}(i) = (-1)^{(a+b-1)/4}$  (Prop. 9.8.6).

From the first part of this proof,  $\chi_{a+b}(1+i) = i^{(a+b-1)/4}$ , so

$$\begin{aligned} \chi_{a+b}(\pi) &= \chi_{a+b}(-1)\chi_{a+b}(a)\chi_{a+b}(i)\chi_{a+b}(1+i) \\ &= (-1)^{(a+b-1)/4} i^{(a+b-1)/4} \\ &= i^{(a+b-1)/2} i^{(a+b-1)/4} \\ &= i^{3(a+b-1)/4} \end{aligned}$$

Conclusion : if  $\pi = a + bi$  is a primary irreducible, such that  $a \wedge b = 1$ , then

$$\chi_\pi(a)\chi_\pi(1+i) = i^{3(a+b-1)/4}$$

□

**Ex. 9.36** Remove the restriction  $(a, b) = 1$  in Exercise 9.34.

*Proof.* Suppose that  $q = a \wedge b > 1$ . Then  $a = qa'$ ,  $b = qb'$ ,  $a', b' \in \mathbb{Z}$ , so  $\pi = q(a' + ib')$ .

As  $\pi$  is irreducible, and as  $q$  is not an unit,  $u = a' + b'i$  is an unit, and so  $\pi = uq$  is associate to  $q$  : the rational integer  $q$  is then a prime in  $D$ , so a rational prime  $q \equiv 3 \pmod{4}$ .

If  $u = \pm i$ , then  $\pi = \pm q = a + bi$  is such that  $b$  is odd, in contradiction with  $\pi$  primary. Thus  $u = \pm 1$ , and  $\pi = \varepsilon q$ ,  $\varepsilon = \pm 1$ . As  $\pi$  is primary,  $\varepsilon = -1$ , so  $\pi = -q$ .

Then  $\chi_\pi(a) = \chi_{-q}(-q) = 0$ , the result of Ex. 34 is false if  $b = 0$ .

Conclusion : if  $\pi = a + bi$  is a primary irreducible, and  $b \neq 0$ , then

- (a) if  $\pi \equiv 1 \pmod{4}$ ,  $\chi_\pi(a) = i^{(a-1)/2}$ ,
- (b) if  $\pi \equiv 3 + 2i \pmod{4}$ ,  $\chi_\pi(a) = -i^{(-a-1)/2}$ .

□

**Ex. 9.37** Combine Exercises 32, 33, 34, and 35 to show  $\chi_\pi(1+i) = i^{(a-b-b^2-1)/4}$ . Show that this result implies Exercise 26 of Chapter 5 “the biquadratic character of 2”).

**Lemma.** If  $\pi = a + bi$  is a primary prime, then

$$\chi_\pi(i) = i^{\frac{-a+1}{2}}.$$

*Proof.* (of Lemma.) Let  $\pi = a + bi$  a primary prime in  $\mathbb{Z}[i]$ .

- If  $\pi = -q$ , where  $q \equiv 3 \pmod{4}$ ,  $q > 0$  is a rational prime, then  $a = -q$ ,  $b = 0$ . By definition of the quartic character,

$$\chi_q(i) = i^{\frac{N(q)-1}{4}} = i^{\frac{q^2-1}{4}}.$$

Write  $-q = a = 4k + 1$ ,  $k \in \mathbb{Z}$ . Then

$$\begin{aligned} \frac{q^2-1}{4} &= 4k^2 + 2k \\ &\equiv 2k = \frac{a-1}{2} \pmod{4}. \end{aligned}$$

Therefore

$$\chi_{-q}(i) = \chi_q(i) = i^{\frac{q^2-1}{4}} = i^{\frac{a-1}{2}} = \left(\frac{1}{i}\right)^{\frac{-a+1}{2}} = (-i)^{\frac{-a+1}{2}} = (-1)^{\frac{-a+1}{2}} i^{\frac{-a+1}{2}} = i^{\frac{-a+1}{2}},$$

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

Suppose now that  $N(\pi) = p$ , where  $p \equiv 1 \pmod{4}$  is a rational prime. Then

$$\chi_\pi(i) = i^{\frac{N(\pi)-1}{4}} = i^{\frac{p-1}{4}}.$$

Since  $\pi = a + bi$  is primary, there are two cases.

- If  $a \equiv 1 \pmod{4}$ ,  $b \equiv 0 \pmod{4}$ , then  $a = 4A + 1$ ,  $b = 4B$ ,  $A, B \in \mathbb{Z}$ .

$$\begin{aligned} \frac{p-1}{4} &= \frac{a^2 + b^2 - 1}{4} \\ &= \frac{16A^2 + 8A + 16B^2}{4} \\ &= 4A^2 + 2A + 4B^2 \\ &\equiv 2A = \frac{a-1}{2} \end{aligned}$$

Therefore

$$\chi_\pi(i) = i^{\frac{p-1}{4}} = i^{\frac{a-1}{2}} = \left(\frac{1}{i}\right)^{\frac{-a+1}{2}} = (-i)^{\frac{-a+1}{2}} = (-1)^{\frac{-a+1}{2}} i^{\frac{-a+1}{2}} = i^{\frac{-a+1}{2}},$$

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

- If  $a \equiv 3 \pmod{4}, b \equiv 2 \pmod{4}$ , then  $a = 4A - 1, b = 4B + 2, A, B \in \mathbb{Z}$ .

$$\begin{aligned} \frac{p-1}{4} &= \frac{a^2 + b^2 - 1}{4} \\ &= \frac{16A^2 - 8A + 16B^2 + 16B + 4}{4} \\ &= 4A^2 - 2A + 4B^2 + 4B + 1 \\ &\equiv -2A + 1 = \frac{-a+1}{2} \pmod{4} \end{aligned}$$

Therefore  $\chi_\pi(i) = (-1)^{\frac{-a+1}{4}}$ .

The equality  $\chi_\pi(i) = (-1)^{\frac{-a+1}{4}}$  is verified for all primary primes  $\pi$ .

□

*Proof.* (of Ex.9.37) Let  $\pi = a + ib$  be a primary irreducible in  $\mathbb{Z}[i]$ .

- If  $b = 0$ , then  $\pi = a \in \mathbb{Z}$ . As  $\pi$  is primary,  $\pi = -q, q \equiv 3 \pmod{4}$ , where  $q$  is a rational prime, so  $a = -q, b = 0$ . By Ex. 9.32 (or its generalization 9.35),

$$\chi_\pi(1+i) = \chi_{-q}(1+i) = i^{(-q-1)/4} = i^{(a-b-b^2-1)/4}.$$

- If  $b \neq 0$ , then  $a \wedge b = 1$  (see Ex. 9.36), and by Ex. 9.35,

$$\chi_\pi(a)\chi_\pi(1+i) = i^{3(a+b-1)/4}.$$

- If  $\pi \equiv 1 [4], a \equiv 1 [4], b \equiv 0 [4] : a = 4A + 1, b = 4B, A, B \in \mathbb{Z}$ .  
By Ex. 9.34(a),

$$\chi_\pi(a) = i^{(a-1)/2}, \chi_\pi(a)^{-1} = (-i)^{(a-1)/2} = i^{(a-1)/2}.$$

$$\begin{aligned} \chi_\pi(1+i) &= i^{3\frac{a+b-1}{4} - 2\frac{a-1}{4}} \\ &= i^{\frac{a+3b-1}{4}} \\ &= i^{\frac{a-b-b^2-1}{4}}, \end{aligned}$$

$$\text{since } \left(\frac{a+3b-1}{4}\right) - \left(\frac{a-b-b^2-1}{4}\right) = b + \frac{b^2}{4} = 4B + 4B^2 \equiv 0 [4].$$

- If  $\pi \equiv 3 + 2i [4], a \equiv 3 [4], b \equiv 2 [4] : a = 4A - 1, b = 4B + 2, A, B \in \mathbb{Z}$ .  
By Ex. 9.34(b),

$$\chi_\pi(a) = -i^{(-a-1)/2}, \chi_\pi(a)^{-1} = -i^{(a+1)/2} = i^{(a-3)/2},$$

so

$$\chi_\pi(1+i) = i^{(3a+3b-3+2a-6)/4} = i^{(5a+3b-9)/4}.$$

$$\text{Now } \frac{1}{4}[(a-b-b^2-1) - (5a+3b-9)] = \frac{1}{4}(-4a-4b-b^2+8) = -a-b+2-\frac{b^2}{4} = -4A+1-4B-2+2-(2B+1)^2 \equiv 0 [4],$$

$$\text{thus } \chi_\pi(1+i) = i^{(a-b-b^2-1)/4}.$$

Conclusion : if  $\pi = a + ib$  is primary irreducible, then

$$\chi_\pi(1+i) = i^{(a-b-b^2-1)/4}$$

Second part : the biquadratic character of 2 (see Ex. 5.25 to 5.28).

Let  $p \equiv 1 \pmod{4}$ . Then  $p = N(\pi)$ , where  $\pi = a + bi$  is a primary prime.

We show first that  $\chi_\pi(2) = i^{\frac{ab}{2}}$ .

Since  $2 = i^3(1+i)^2$ , the first part of the exercise, and the Lemma, give

$$\begin{aligned}\chi_\pi(2) &= \chi_\pi(i)^3 \chi_\pi(1+i)^2 \\ &= i^{\frac{3(-a+1)}{2}} i^{\frac{a-b-b^2-1}{2}} \\ &= i^{1-a-(b+1)\frac{b}{2}}\end{aligned}$$

Since  $\pi$  is primary,  $a \equiv b+1 \equiv -b+1 \pmod{4}$ , therefore

$$\begin{aligned}1-a-(b+1)\frac{b}{2} &\equiv -b-(b+1)\frac{b}{2} \\ &\equiv \frac{b}{2}(-b-3) \\ &\equiv \frac{b}{2}(-b+1) \\ &\equiv \frac{ab}{2} \pmod{4},\end{aligned}$$

so  $\chi_\pi(2) = i^{\frac{ab}{2}}$ .

Now we show that  $p$  is of the form  $p = A^2 + 64b^2$  if and only if  $p \equiv 1 \pmod{4}$  and if  $x^4 \equiv 2$  has a solution  $x \in \mathbb{Z}$ .

If  $p = A^2 + 64B^2 = A^2 + (8B)^2$ , then the prime number  $p$  is a sum of two squares, and  $p \neq 2$ , therefore  $p \equiv 1 \pmod{4}$ . Since  $p = A^2 + 64b^2$ ,  $A$  is odd. Put  $b = 8B$ , and  $a = A$  if  $A \equiv 1 \pmod{4}$ ,  $a = -A$  if  $A \equiv -1 \pmod{4}$ . Then  $\pi = a + bi$  is such that  $N(\pi) = a^2 + b^2 = p$ , and  $a \equiv 1, b \equiv 0 \pmod{4}$ , therefore  $\pi$  is a primary prime. Then

$$\chi_\pi(2) = i^{\frac{ab}{2}} = i^{4aB} = 1.$$

Therefore there exists  $\alpha \in D$  such that  $2 \equiv \alpha^4 \pmod{\pi}$ . As  $D/\pi D$  is the set of classes of  $0, 1, \dots, p-1$ , there exists  $x \in \mathbb{Z}$  such that  $x \equiv \alpha \pmod{\pi}$ , so  $2 \equiv x^4 \pmod{\pi}$ .

Then  $p = N(\pi) \mid N(x^4 - 2) = (x^4 - 2)^2$ , thus  $p \mid x^4 - 2$ , in other words  $2 \equiv x^4 \pmod{p}$ .

Conversely, suppose that  $p \equiv 1 \pmod{4}$  and that 2 is a biquadratic residue modulo  $p$ . As  $p \equiv 1 \pmod{4}$ ,  $p = \pi\bar{\pi}$ , where  $\pi = a + bi$  is a primary prime. Since  $2 \equiv x^4 \pmod{p}$  for some  $x \in \mathbb{Z}$ , then  $2 \equiv x^4 \pmod{\pi}$ , so  $\chi_\pi(2) = 1$ . Moreover

$$1 = \chi_\pi(2) = i^{\frac{ab}{2}}.$$

Since  $a$  is odd,  $8 \mid b$ , therefore  $p = A^2 + 64b^2$ , where  $A = a, B = b/8$ .

Conclusion :

$$\exists(A, B) \in \mathbb{Z}^2, p = A^2 + 64B^2 \iff (p \equiv 1 \pmod{4} \text{ and } \exists x \in \mathbb{Z}, x^4 \equiv 2 \pmod{p}).$$

□

**Ex. 9.38** Prove part (d) of Proposition 9.8.3.

**Proposition 9.8.3(d)** If  $\pi$  is a primary irreducible then  $\chi_\pi(-1) = (-1)^{(a-1)/2}$ , where  $\pi = a + bi$ .

*Proof.* Let  $\pi = a + bi$  a primary irreducible. Then  $a$  is odd, and  $b$  is even, and  $N(\pi) = a^2 + b^2$ . Then

$$\chi_\pi(-1) = (-1)^{\frac{N(\pi)-1}{4}} = (-1)^{\frac{a^2-1}{4} + \frac{b^2}{4}} = [(-1)^{\frac{a+1}{2}}]^{\frac{a-1}{2}} (-1)^{\frac{b^2}{4}}.$$

By Lemma 6, section 7,  $a \equiv 1 \pmod{4}$ ,  $b \equiv 0 \pmod{4}$ , or  $a \equiv 3 \pmod{4}$ ,  $b \equiv 2 \pmod{4}$ .

- If  $a \equiv 1 \pmod{4}$ ,  $b \equiv 0 \pmod{4}$ , then  $(-1)^{\frac{a+1}{2}} = -1$ ,  $(-1)^{\frac{b^2}{4}} = +1$ , so

$$\chi_\pi(-1) = (-1)^{\frac{a-1}{2}}.$$

- If  $a \equiv 3 \pmod{4}$ ,  $b \equiv 2 \pmod{4}$ , then  $(-1)^{\frac{a+1}{2}} = 1$ ,  $(-1)^{\frac{b^2}{4}} = -1$ , so

$$\chi_\pi(-1) = -1 = (-1)^{\frac{a-1}{2}}.$$

Conclusion: if  $\pi$  is a primary irreducible in  $\mathbb{Z}[i]$ , then

$$\chi_\pi(-1) = (-1)^{(a-1)/2}.$$

□

**Ex. 9.39** Let  $p \equiv 1 \pmod{6}$  and write  $4p = A^2 + 27B^2$ ,  $A \equiv 1 \pmod{3}$ . Put  $m = (p-1)/6$ . Show  $\binom{3m}{m} \equiv -1 \pmod{p} \iff 2 \mid B$ .

*Proof.* Let  $p$  be a rational prime,  $p \equiv 1 \pmod{6}$ . As  $p \equiv 1 \pmod{3}$ , we know from Theorem 2, Chapter 8, that there are integers  $A$  and  $B$  such that  $4p = A^2 + 27B^2$ ,  $A \equiv 1 \pmod{3}$ , and that  $A$  is uniquely determined by these conditions.

Then  $A, B$  have same parities. If we take  $a = \frac{A+3B}{2}$ ,  $b = 3B$ , then  $A = 2a - b$ ,  $B = \frac{b}{3}$ , and  $4p = (2a - b)^2 + 3b^2$ , so  $p = a^2 - ab + b^2$ . If  $\pi = a + b\omega$ , then  $N(\pi) = p$ . Since  $A = 2a - b \equiv 1 \pmod{3}$ , and  $b = 3B \equiv 0 \pmod{3}$ , then  $a \equiv -1 \pmod{3}$ , so  $\pi$  is a primary prime.

- Suppose that  $2 \mid B$ . Since  $p = a^2 - ab + b^2$  is odd, and  $b = 3B$ ,

$$2 \mid B \iff 2 \mid b \iff (b \equiv 0 \pmod{2}, a \equiv 1 \pmod{2}) \iff \pi \equiv 1 \pmod{2}.$$

By Proposition 9.6.1,

$$\pi \equiv 1 \pmod{2} \iff x^3 - 2 \text{ is solvable in } D \iff \chi_\pi(2) = 1.$$

Therefore

$$2 \mid B \iff \chi_\pi(2) = 1.$$

Here  $\chi_\pi$  is of order 3, so  $\chi_\pi^2 \neq \varepsilon$ . By Exercise 8.6,

$$J(\chi_\pi, \chi_\pi) = \chi_\pi(2)^{-2} J(\chi_\pi, \rho),$$

where  $\rho$  is the Legendre's character.

In this case,  $2 \mid B$ ,  $\chi_\pi(2) = 1$ , so  $J(\chi_\pi, \chi_\pi) = J(\chi_\pi, \rho)$ , and by Lemma 1 section 4, where  $p \equiv 1 \pmod{3}$  and  $p = N(\pi)$ ,

$$\pi = a + b\omega = J(\chi_\pi, \chi_\pi) = J(\chi_\pi, \rho).$$

By Exercise 8.15,

$$N(y^2 = x^3 + 1) = p + A,$$

and the Exercise 8.27(b) gives

$$N(y^2 = x^3 + 1) = N(y^2 + x^3 = 1) = p + 2 \operatorname{Re} J(\chi_\pi, \rho).$$

thus

$$A = 2 \operatorname{Re} J(\chi_\pi, \rho) = 2 \operatorname{Re} \pi = 2a - b.$$

Moreover, since  $J(\chi_\pi, \rho) = \pi = a + b\omega$ , by Exercise 8.27(c),

$$2a - b \equiv -\binom{(p-1)/2}{(p-1)/3}.$$

Therefore

$$-A \equiv \binom{(p-1)/2}{(p-1)/3} = \binom{(p-1)/2}{(p-1)/2 - (p-1)/6} = \binom{(p-1)/2}{(p-1)/6} = \binom{3m}{m} \pmod{p},$$

where  $m = (p-1)/6$ . Since  $A \equiv 1 \pmod{3}$ ,

$$\binom{3m}{m} \equiv -1 \pmod{p}.$$

• Conversely, suppose that  $\binom{3m}{m} \equiv -1 \pmod{p}$ . Then  $A = 2a - b \equiv -\binom{3m}{m} \pmod{p}$ . Write  $J(\chi_\pi, \rho) = c + d\omega$ . By Exercise 8.27(c),  $2c - d \equiv -\binom{3m}{m} \pmod{p}$ . thus

$$2a - b \equiv 2c - d \pmod{p}.$$

Since  $|J(\chi_\pi, \rho)| = \sqrt{p}$ ,

$$4p = (2a - b)^2 + 3b^2 = (2c - d)^2 + 3d^2,$$

thus  $d \equiv \pm b \pmod{p}$ .

By Exercise 8.6,

$$\pi = J(\chi_\pi, \chi_\pi) = \chi_\pi(2)^{-2} J(\chi_\pi, \rho),$$

Here  $\chi_\pi$  is of order 3, therefore  $\chi_\pi(2)^{-2} = \chi_\pi(2) \in \{1, \omega, \omega^2\}$ , so

$$\pi = J(\chi_\pi, \chi_\pi) = \chi_\pi(2) J(\chi_\pi, \rho).$$

If  $\chi_\pi(2) = \omega$ , then  $a + b\omega = \omega(c + d\omega) = -d + \omega(c - d)$ . Then  $a = -d \equiv \pm b \pmod{p}$ . As  $a \equiv -b\omega \pmod{\pi}$ , we would have  $-b\omega \equiv \pm b \pmod{\pi}$ . Here  $\pi \nmid b$ , otherwise  $p = N(\pi) \mid N(b) = b^2$ , so  $p \mid b$ , and  $p = a^2 - ab + b^2$ , so  $p \mid a$ , and  $p^2 \mid p$ , which is a nonsense. Therefore  $\pi \mid \omega \pm 1$ , where  $\pi$  is a primary prime: it's impossible. Indeed  $\omega + 1$  is a unit and  $\omega - 1$  is prime, so  $\pi \mid \omega - 1 = -\lambda$  implies that  $\pi$  and  $\lambda$  are associate, in contradiction with  $N(\pi) = p \neq 3 = N(\lambda)$ .

If  $\chi_\pi(2) = \omega^2$ , then  $a + b\omega = \omega^2(c + d\omega) = (d - c) - \omega c$ , so  $a = d - c, b = -c$ .

Reasoning modulo  $\bar{\pi} = a + b\omega^2 = (a - b) + b\omega$ , where  $\bar{\pi} \mid \pi\bar{\pi} = p$ , we obtain

$$d = a - b \equiv -b\omega \pmod{\bar{\pi}},$$

where  $d \equiv \pm b \pmod{\bar{\pi}}$ , so  $-b\omega \equiv \pm b \pmod{\bar{\pi}}$ . Since  $N(\bar{\pi}) = p$ , we obtain the same contradiction as above.

So  $\chi_\pi(2) = 1$ , and the previously proved equivalence  $2 \mid B \iff \chi_\pi(2) = 1$  show that  $2 \mid B$ .

Conclusion:

$$\binom{(p-1)/2}{(p-1)/6} \equiv -1 \pmod{p} \iff 2 \mid B.$$

□

**Ex. 9.40** Let  $p \equiv 1 \pmod{6}$ , and put  $p = \pi\bar{\pi}$  where  $\pi$  is primary. Write  $\pi = a + b\omega$  and show

(a) If  $\chi_\pi(2) = \omega$  then  $2b - a \equiv -\binom{3m}{m} \pmod{p}$ .

(b) If  $\chi_\pi(2) = \omega^2$  then  $a + b \equiv \binom{3m}{m} \pmod{p}$ .

(c) If  $\chi_\pi(2) = \omega$  put  $A = 2a - b, B = b/3$ . Show  $(A - 9B)/2 \equiv \binom{3m}{m} \pmod{p}$ .

(d) If  $\chi_\pi(2) = \omega^2$  put  $2a - b = A$  and  $B = -b/3$ . Show  $(A - 9B)/2 \equiv \binom{3m}{m} \pmod{p}$ .

(e) Show that the “normalization” of  $B$  in (c) and (d) is equivalent to  $A \equiv B \pmod{4}$ .  
[Recall  $\chi_\pi(2) \equiv \pi \pmod{2}$  by cubic reciprocity.]

*Proof.* Here  $p = 6m + 1, m \in \mathbb{Z}$ , and  $p = \pi\bar{\pi}$ , where  $\pi = a + b\omega$  is a primary prime.

We have proved in Exercise 39 that

$$\pi = J(\chi_\pi, \chi_\pi) = \chi_\pi(2)J(\chi_\pi, \rho). \quad (1)$$

Write  $J(\chi_\pi, \rho) = c + d\omega$ . The Exercise 8.27(c) shows that

$$2c - d \equiv -\binom{3m}{m} \pmod{p}. \quad (2)$$

(a) If  $\chi_\pi(2) = \omega$ , then (1) gives

$$a + b\omega = \omega(c + d\omega) = -d + \omega(c - d),$$

so  $a = -d, b = c - d$ , therefore the equality (2) gives

$$2b - a = 2(c - d) + d = 2c - d \equiv -\binom{3m}{m} \pmod{p}.$$

(b) If  $\chi_\pi(2) = \omega^2$ , then

$$a + b\omega = \omega^2(c + d\omega) = d - c - c\omega,$$

so  $a = d - c, b = -c$ , and

$$a + b = d - 2c \equiv \binom{3m}{m} \pmod{p}.$$

(c) Suppose that  $\chi_\pi(2) = \omega$ , and put  $A = 2a - b, B = b/3$ , so

$$4p = A^2 + 27B^2, \quad A \equiv 1 \pmod{3},$$

which shows that  $A, B$  have same parities. Then, by part (a),

$$\begin{aligned} \frac{A - 9B}{2} &= \frac{2a - b - 3b}{2} \\ &= a - 2b \\ &\equiv \binom{3m}{m} \pmod{p} \end{aligned}$$

(d) Suppose that  $\chi_\pi(2) = \omega^2$ , and put  $A = 2a - b, B = -b/3$ , so we have again

$$4p = A^2 + 27B^2, \quad A \equiv 1 \pmod{3}.$$

In this case, by part (b)

$$\begin{aligned} \frac{A - 9B}{2} &= \frac{2a - b + 3b}{2} \\ &= a + b \\ &\equiv \binom{3m}{m} \pmod{p} \end{aligned}$$

(e) The conditions  $4p = A^2 + 27B^2, A \equiv 1 \pmod{3}$ , determine  $A, B$ , except the sign of  $B$ . So  $4p = A^2 + 27B^2 = (2a - b)^2 + 3b^2$ , implies  $A = 2a - b$  and  $B = \pm \frac{b}{3}$ .

By Exercise 39, since  $A, B$  have same parity, the condition  $A, B$  odd is equivalent to  $\chi_\pi(2) \in \{\omega, \omega^2\}$ . We choose this sign of  $B$  so that

$$\frac{A - 9B}{2} \equiv \binom{3m}{m} \pmod{p}.$$

By parts (d) and (e), where  $A, B$  are odd, this choice is given by  $B = b/3$  if  $\chi_\pi(2) = \omega$ , and  $B = -b/3$  if  $\chi_\pi(2) = \omega^2$ . We show that these conditions are equivalent to  $A \equiv B \pmod{4}$ .

• If  $\chi_\pi(2) = \omega$ , then  $A = 2a - b, B = b/3$ .

By cubic reciprocity,  $\chi_\pi(2) \equiv \pi \pmod{2}$  (see section 6). Here  $\chi_\pi(2) = \omega$ , so  $\omega \equiv a + b\omega \pmod{2}$ , therefore  $a \equiv 0 \pmod{2}, b \equiv 1 \pmod{2}$ ,

$$A = 2a - b \equiv -b \equiv \frac{b}{3} = B \pmod{4},$$

so  $A \equiv B \pmod{4}$ .

• If  $\chi_\pi(2) = \omega^2$ , then  $A = 2a - b, B = -b/3$ . In this case,

$$\omega^2 = -1 - \omega \equiv a + b\omega \pmod{2},$$

therefore  $a \equiv 1 \equiv b \pmod{2}$ , and

$$A = 2a - b \equiv 2 - b \equiv b \equiv -\frac{b}{3} = B \pmod{4}.$$



In both cases, the choice of the sign of  $B$  implies that  $A \equiv B \pmod{4}$ .

Conversely, suppose that  $A \equiv B \pmod{4}$ . Write  $B = \varepsilon \frac{b}{3}$ , where  $\varepsilon = \pm 1$ . Then  $A \equiv B \pmod{4}$  gives

$$2a - b \equiv \varepsilon \frac{b}{3} \equiv -\varepsilon b \pmod{4},$$

thus  $a \equiv \frac{1-\varepsilon}{2}b \pmod{2}$ . Then

$$\begin{aligned}\chi_\pi(2) &\equiv \pi = a + b\omega \\ &\equiv b \left( \frac{1-\varepsilon}{2} + \omega \right) \pmod{2}\end{aligned}$$

If  $\chi_\pi(2) = \omega$ , since  $b = 3B$  is odd,  $\frac{1-\varepsilon}{2} \equiv 0 \pmod{2}$ , therefore  $\varepsilon = 1$ , and  $B = \frac{b}{3}$ .

If  $\chi_\pi(2) = \omega^2 = -1 - \omega$ ,  $\frac{1-\varepsilon}{2} \equiv 1 \pmod{2}$ , therefore  $\varepsilon = -1$ , and  $B = -\frac{b}{3}$ .

The normalisation given in parts (c) and (d) for the choice of the sign of  $B$  is equivalent to  $A \equiv B \pmod{4}$  (where  $A, B$  are odd).

□

**Ex. 9.41** Let  $p \equiv 1 \pmod{6}$ ,  $4p = A^2 + 27B^2$ ,  $A \equiv 1 \pmod{3}$ ,  $A$  and  $B$  odd. Put  $\pi = a + b\omega$ ,  $2a - b = A$ ,  $b = 3B$ . Let  $\chi_\pi$  be the cubic residue character.

- (a) If  $\chi_\pi(2) = \omega$  show  $N(x^3 + 2y^3 = 1) = p + 1 + 2b - a \equiv 0 \pmod{2}$ .
- (b) If  $\chi_\pi(2) = \omega^2$  show  $N(x^3 + 2y^3 = 1) = p + 1 - a - b \equiv 0 \pmod{2}$ .
- (c) Show that if  $A \equiv B \pmod{4}$ , then assuming  $\chi_\pi(2) \neq 1$ , one has  $\chi_\pi(2) = \omega$ .
- (d) If  $\chi_\pi(2) \neq 1$ ,  $A \equiv B \pmod{4}$  then

$$2^{(p-1)/3} \equiv (-A - 3B)/6B \equiv (A + 9B)/(A - 9B) \pmod{\pi}.$$

(This generalization of Euler's criterion is due to E. Lehmer [174]. See also K. Williams [243].)

*Proof.* With the help of Theorem 1, Chapter 8, we obtain, writing  $\chi_\pi(2) = \omega^k$ ,

$$\begin{aligned}
N(x^3 + 2y^3 = 1) &= \sum_{a+2b=1} N(x^3 = a)N(y^3 = b) \\
&= \sum_{a+2b=1} \left( \sum_{i=0}^2 \chi_\pi^i(a) \right) \left( \sum_{j=0}^2 \chi_\pi^j(b) \right) \\
&= \sum_{i=0}^2 \sum_{j=0}^2 \sum_{a+2b=1} \chi_\pi^i(a) \chi_\pi^j(b) \\
&= \sum_{i=0}^2 \sum_{j=0}^2 \sum_{a+b'=1} \chi_\pi^i(a) \chi_\pi^j(2^{-1}b') \\
&= \sum_{i=0}^2 \sum_{j=0}^2 \chi_\pi(2)^{-j} J(\chi_\pi^i, \chi_\pi^j) \\
&= \sum_{i=0}^2 \sum_{j=0}^2 \omega^{-kj} J(\chi_\pi^i, \chi_\pi^j) \\
&= p + \omega^{-k} J(\chi_\pi^2, \chi_\pi) + \omega^{-2k} J(\chi_\pi, \chi_\pi^2) \\
&\quad + \omega^{-k} J(\chi_\pi, \chi_\pi) + \omega^{-2k} J(\chi_\pi^2, \chi_\pi^2) \\
&= p - \omega^{-k} \chi_\pi(-1) - \omega^{-2k} \chi_\pi(-1)^2 + 2 \operatorname{Re}(\omega^{-k} J(\chi_\pi, \chi_\pi)) \\
&= p - \omega^{-k} - \omega^{-2k} + 2 \operatorname{Re}(\omega^{-k} J(\chi_\pi, \chi_\pi)).
\end{aligned}$$

(a) If  $\chi_\pi(2) = \omega$ , then  $k = 1$ . Using  $\chi_\pi^2 = \chi_\pi^{-1} = \overline{\chi_\pi}$ , we obtain

$$\begin{aligned}
N(x^3 + 2y^3 = 1) &= p + 1 + 2 \operatorname{Re}(\omega^2 J(\chi_\pi, \chi_\pi)) \\
&= p + 1 + 2 \operatorname{Re}(\omega^2 \pi),
\end{aligned}$$

since  $J(\chi_\pi, \chi_\pi) = \pi$  (Lemma 1, section 4).

$$\begin{aligned}
\omega^2 \pi &= \omega^2(a + b\omega) = b - a - \omega a, \\
2 \operatorname{Re}(\omega^2 \pi) &= (b - a - \omega a) + (b - a - \omega^2 a) = 2b - 2a + a = 2b - a,
\end{aligned}$$

therefore

$$N(x^3 + 2y^3 = 1) = p + 1 + 2b - a \quad (\text{if } \chi_\pi(2) = \omega).$$

Since in then case  $\chi_\pi(2) = \omega$ , then  $a \equiv 0 \pmod{2}$  (see Ex. 39, part (e)), so  $p + 1 + 2b - a \equiv 0 \pmod{2}$ .

(b) If  $\chi_\pi(2) = \omega^2 = \omega^{-1}$ , then  $k = -1$ , and

$$N(x^3 + 2y^3 = 1) = p + 1 + 2 \operatorname{Re}(\omega \pi),$$

with

$$\begin{aligned}
\omega \pi &= \omega(a + b\omega) = -b + (a - b)\omega, \\
2 \operatorname{Re}(\omega \pi) &= (-b + (a - b)\omega) + (-b + (a - b)\omega^2) = -2b - (a - b) = -a - b,
\end{aligned}$$

therefore

$$N(x^3 + 2y^3 = 1) = p + 1 - a - b \quad (\text{if } \chi_\pi(2) = \omega^2).$$

(c) Suppose that  $A \equiv B \pmod{4}$ , and  $\chi_\pi(2) \neq 1$ . By hypothesis,  $b = 3B$ , and this implies by Exercise 40 (e) that  $\chi_\pi(2) = \omega$  (if not,  $\chi_\pi(2) = \omega^2$ , and  $A \equiv B \pmod{4}$  gives  $B = -b/3$ ).

(d) Suppose that  $\chi_\pi(2) \neq 1, A \equiv B \pmod{4}$ . By part (c),  $\chi_\pi(2) = \omega$ .

Since  $2a - b = A, B = b/3$ , then  $a = \frac{A+3B}{2}, b = 3B$ .

Starting from  $a + b\omega \equiv 0 \pmod{\pi}$ , we obtain

$$3B\omega \equiv -\frac{A+3B}{2} \pmod{\pi}.$$

Since  $pa = a^2 - ab + b^2$ ,  $a$  is relatively prime with  $p$ , therefore  $\pi \nmid b = 1$ , so  $\pi \nmid B = 1$ , and  $\pi \nmid 6 = 1$ , since  $p \equiv 1 \pmod{6}$ , thus

$$\chi_\pi(2) = \omega \equiv \frac{-A-3B}{6B} \pmod{\pi},$$

where we must read in this fraction the product of  $A+3B$  by the inverse modulo  $p$  of  $6B$ . By definition, using  $N(\pi) = p$ ,

$$\chi_\pi(2) \equiv 2^{\frac{p-1}{3}} \pmod{\pi},$$

so

$$2^{\frac{p-1}{3}} \equiv \frac{-A-3B}{6B} \pmod{\pi}.$$

Moreover, since  $4p = A^2 + 27B^2$ ,  $A^2 + 27B^2 \equiv 0 \pmod{p}$ , therefore

$$6B(A+9B) + (A+3B)(A-9B) \equiv 0 \pmod{p}.$$

If  $p \mid A-9B$ , since  $p \nmid 6B$ , this equality implies that  $p \mid A+9B$ , therefore  $p \mid (A-9B) + (A+9B) = 2A$ , which is false. Therefore  $A-9B \not\equiv 0 \pmod{p}$ , and

$$2^{\frac{p-1}{3}} \equiv \frac{-A-3B}{6B} \equiv \frac{A+9B}{A-9B} \pmod{\pi}.$$

□

Note : By a usual argument, if  $h \in \mathbb{Z}$ ,  $2^{\frac{p-1}{3}} \equiv h \pmod{\pi} \iff 2^{\frac{p-1}{3}} \equiv h \pmod{p}$ . Note that the hypothesis  $\chi_\pi(2) \neq 1$  means that 2 is not a cubic residue modulo  $p$ , which is equivalent to  $A, B$  odd by Exercise 39. We can conclude

*Suppose that  $p \equiv 1 \pmod{6}$ , and let  $(A, B)$  be the unique solution of  $4p = A^2 + 27B^2$  such that  $A \equiv 1 \pmod{3}$ , and  $B \equiv A \pmod{4}$  if  $B$  odd, and  $B > 0$  otherwise.*

*If  $B$  is even, then 2 is a cubic residue modulo  $p$ , and  $2^{\frac{p-1}{3}} = 1$ .*

*If  $B$  is odd, then 2 is not a cubic residue modulo  $p$ , and  $B$  satisfies  $B \equiv A \pmod{4}$ .*

*Writing  $a = \frac{A+3B}{2}, b = 3B$ , and  $\pi = a + b\omega$ , then  $\chi_\pi(2) = \omega$ , and*

$$2^{\frac{p-1}{3}} \equiv \frac{A+9B}{A-9B} \pmod{p}.$$

The three roots of  $x^3 - 1$  in  $\mathbb{F}_p$  are  $1, \frac{A+9B}{A-9B}, \frac{A-9B}{A+9B}$ . Here 2 is not a cubic residue modulo  $p$ , and  $2^{\frac{p-1}{3}}$  is also a cubic root of unity modulo  $p$ , so  $2^{\frac{p-1}{3}} \equiv \frac{A+9B}{A-9B} \pmod{p}$ . The proposition explicits the choice of the sign of  $B$  which gives  $2^{\frac{p-1}{3}} \equiv \frac{A-9B}{A+9B} \pmod{p}$ .

Numerical example : Let  $p$  be the prime 967. If we decompose  $p$  on the form  $p = \pi\bar{\pi}$ , we obtain  $\pi = a + b\omega = -34 - 27\omega$ . To obtain these result without tries, I find  $k = 682$  such that  $p \mid k^2 + 3$  with the Tonelli-Shanks algorithm, and I compute  $\gcd(p, k+1+2\omega) = a + b\omega$ , where  $a + b\omega$  is primary, with a small Python program using the class of elements in  $\mathbb{Z}[\omega]$  and the Euclid algorithm in  $\mathbb{Z}[\omega]$ . This gives the decompositions

$$967 = p = a^2 - ab + b^2 = 34^2 - 34 \times 27 + 27^2,$$

and

$$3868 = 4p = (2a - b)^2 + 3b^2 = A^2 + 27B^2 = 41^2 + 27 \times 9^2,$$

where  $A \equiv 1 \pmod{3}$ , and I choose the sign of  $B$  such that  $B \equiv A \pmod{4}$ . We obtain  $A = -41, B = -9$ , and  $a, b$  must verify  $A = 2a - b, B = b/3$ .

Then  $\chi_\pi(2) = \omega$ , where  $\pi = -41 - 9\omega$ . In  $\mathbb{F}_{967}$ , the cubic roots of unity modulo  $p$  are  $1, 142, 824$ :  $142^3 \equiv 824^3 \equiv 1 \pmod{967}$ .

Here  $(A + 9B)(A - 9B)^{-1} = 142$ , and we verify with a fast exponentiation that  $2^{\frac{p-1}{3}} = 2^{322} \equiv 142 \pmod{967}$ .

I give here an extract of a table obtained with this program, which for each  $p$  gives  $A, B$  such that  $4p = A^2 + 27B^2$ ,  $A \equiv 1 \pmod{3}$  and such that  $B \equiv A \pmod{4}$  if  $A, B$  odd, and  $\pi = a + b\omega$  satisfies  $\chi_\pi(2) = \omega$  (or  $\chi_\pi(2) = 1$  if  $A, B$  even, which corresponds to the case  $a \equiv 1, b \equiv 0 \pmod{2}$ ).

$p$	$A$	$B$	$\pi = a + b\omega$	$a \% 2$	$b \% 2$	$2^{\frac{p-1}{3}} \% p$	$\frac{A-9B}{A+9B}$	$\chi_\pi(2)$
787	31	-9	$2 - 27\omega$	0	1	379	379	$\omega$
811	-56	-2	$-31 - 6\omega$	1	0	1	130	1
823	-5	11	$14 + 33\omega$	0	1	648	648	$\omega$
829	7	11	$20 + 33\omega$	0	1	125	125	$\omega$
853	-35	9	$-4 + 27\omega$	0	1	632	632	$\omega$
859	13	-11	$-10 - 33\omega$	0	1	260	260	$\omega$
877	-59	1	$-28 + 3\omega$	0	1	594	594	$\omega$
883	-47	-7	$-34 - 21\omega$	0	1	545	545	$\omega$
907	19	11	$26 + 33\omega$	0	1	384	384	$\omega$
919	52	-6	$17 - 18\omega$	1	0	1	52	1
937	61	1	$32 + 3\omega$	0	1	614	614	$\omega$
967	-41	-9	$-34 - 27\omega$	0	1	142	142	$\omega$
991	61	-3	$26 - 9\omega$	0	1	113	113	$\omega$
997	10	-12	$-13 - 36\omega$	1	0	1	692	1

As a verification I compute  $\chi_\pi(2)$  with a fast exponentiation in  $\mathbb{Z}[\omega]$  :  $\chi_\pi(2) = 2^{\frac{p-1}{3}} \pmod{\pi}$ .

We obtain the primary prime  $\mu$  such that  $N(\mu) = p, \chi_\mu(2) = \omega^2$  by taking the conjugate of  $\pi$ . For instance, with  $p = 787$ ,  $\pi = 2 - 27\omega$  satisfies  $\chi_\pi(2) = \omega$ , therefore  $\chi_{\bar{\pi}}(2) = \chi_{29+27\omega} = \omega^2$ .

The lines where  $\chi_\pi(2) = 1$ , corresponding to the case where  $A, B$  are even (or equivalently  $a$  odd,  $b$  even), give the decomposition  $p = x^2 + 27y^2$ , ( $x = A/2, y = B/2$ ). For instance  $997 = 5^2 + 27 \times 6^2$ . If  $p$  is prime,

$$\exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}, p = x^2 + 27y^2 \iff p \equiv 1 \pmod{3} \text{ and } \exists a \in \mathbb{Z}, 2 \equiv a^3 \pmod{p}.$$

**Ex. 9.42** The notation being as in Section 12 show that the minimal polynomial of  $g(\chi_\pi)$  is  $x^3 - 3px - Ap$ .

Note : we must read “the minimal polynomial of  $G = g(\chi_\pi) + \overline{g(\chi_\pi)}$  is  $x^3 - 3px - Ap$ ”.

*Proof.* Write  $f(x) = \sum_{i=0}^3 a_i x^i = x^3 - 3px - Ap$ .

Then  $a_3 = 1$ ,  $p \mid a_0 = Ap$ ,  $p \mid a_1 = -3p$ ,  $p \mid a_2 = 0$ .

Moreover, since  $4p = A^2 + 27B^2$ ,  $p \nmid A$ , therefore  $p^2 \nmid a_0$ .

The Eisenstein's Irreducibility Criterion (Ex. 6.23) shows that  $f(x)$  is irreducible over  $\mathbb{Q}$ . By section 12,  $G$  is a root of  $f$ , so  $f$  is the minimal polynomial of  $G$ .  $\square$

**Ex. 9.43** Find the local maxima and minima of  $x^3 - 3px - Ap$  and show that each of the intervals  $(-2\sqrt{p}, -\sqrt{p})$ ,  $(-\sqrt{p}, \sqrt{p})$ ,  $(\sqrt{p}, 2\sqrt{p})$  contains exactly one of the values  $2\text{Re}(\omega^k g(\chi_\pi))$ ,  $k = 0, 1, 2$ .

*Proof.* Write  $\chi = \chi_\pi$ , and for  $k \in \{0, 1, 2\}$ ,

$$G_k = 2\text{Re}(\omega^k g(\chi)) = \omega^k g(\chi) + \overline{\omega^k g(\chi)},$$

so  $G = G_0$ . As in section 12, since  $g(\chi)^3 = p\pi$ , and  $|g(\chi)|^2 = p$ ,

$$\begin{aligned} G_k^3 &= g(\chi)^3 + \overline{g(\chi)}^3 + 3\omega^{2k} g(\chi)^2 \overline{g(\chi)} + 3\omega^k g(\chi) \overline{\omega^{2k} g(\chi)}^2 \\ &= p\pi + p\overline{\pi} + 3g(\chi)\overline{g(\chi)}(\omega^k g(\chi) + \overline{\omega^k g(\chi)}) \\ &= 3pG_k + p(2a - b) \\ &= 3pG_k + pA \end{aligned}$$

So  $G_0, G_1, G_2$  are the three roots of  $f(x) = x^3 - 3px - Ap$ .

$f'(x) = 3(x^2 - p) < 0$  iff  $-\sqrt{p} < x < \sqrt{p}$ .  $f$  is decreasing on  $[-\sqrt{p}, \sqrt{p}]$ , and increasing on  $] -\infty, -\sqrt{p}[$ , and on  $[\sqrt{p}, +\infty[$ .

Since  $4p = A^2 + 27B^2$ ,  $|A| < 2\sqrt{p}$ , therefore

$$\begin{aligned} f(\sqrt{p}) &= p\sqrt{p} - 3p\sqrt{p} - Ap \\ &= -p(2\sqrt{p} + A) < 0, \end{aligned}$$

and

$$\begin{aligned} f(-\sqrt{p}) &= -p\sqrt{p} + 3p\sqrt{p} - Ap \\ &= p(2\sqrt{p} - A) > 0. \end{aligned}$$

$\square$

Since  $\lim_{x \rightarrow -\infty} f(x) = -\infty$  and  $\lim_{x \rightarrow +\infty} f(x) = +\infty$ , the intermediate value theorem shows that  $f$  has a unique root in each of the intervals  $] -\infty, -\sqrt{p}[$ ,  $[-\sqrt{p}, \sqrt{p}]$ ,  $[\sqrt{p}, +\infty[$ .

Moreover

$$\begin{aligned} f(2\sqrt{p}) &= 8p\sqrt{p} - 6p\sqrt{p} - Ap = p(2\sqrt{p} - A) > 0, \\ f(-2\sqrt{p}) &= -8p\sqrt{p} + 6p\sqrt{p} - Ap = p(-2\sqrt{p} - A) < 0, \end{aligned}$$

therefore  $f$  has a unique root in each of the intervals  $] -2\sqrt{p}, -\sqrt{p}[$ ,  $[-\sqrt{p}, \sqrt{p}]$ ,  $[\sqrt{p}, 2\sqrt{p}[$ .

**Ex. 9.44** Let  $n \in \mathbb{Z}$ ,  $n = s_1 \cdots s_t$ ,  $n \equiv 1 \pmod{4}$ ,  $i = 1, \dots, t$ . Show  $(n-1)/4 \equiv \sum_{i=1}^t (s_i-1)/4 \pmod{4}$ .

*Proof.* If  $n = st$ ,  $s \equiv 1$ ,  $t \equiv 1 \pmod{4}$ , then  $s = 4k+1$ ,  $t = 4l+1$ ,  $k, l \in \mathbb{Z}$ , so

$$n = (4k+1)(4l+1) = 16kl + 4k + 4l + 1, \frac{n-1}{4} = 4kl + k + l \equiv k + l = \frac{s-1}{4} + \frac{t-1}{4} \pmod{4}.$$

Reasoning by induction on  $t$ , suppose that every product of  $t$  factors  $n = s_1 s_2 \cdots s_t$ , where  $s_i \equiv 1 \pmod{4}$  verifies

$$\frac{n-1}{4} \equiv \sum_{i=1}^t \frac{s_i-1}{4} \pmod{4}.$$

If  $n' = s_1 s_2 \cdots s_t s_{t+1} = n s_{t+1}$ ,  $s_i \equiv 1 \pmod{4}$ , then  $n \equiv 1$ ,  $s_{t+1} \equiv 1 \pmod{4}$ , so

$$\frac{n'-1}{4} \equiv \frac{n-1}{4} + \frac{s_{t+1}-1}{4} \equiv \sum_{i=1}^t \frac{s_i-1}{4} + \frac{s_{t+1}-1}{4} \equiv \sum_{i=1}^{t+1} \frac{s_i-1}{4} \pmod{4}.$$

Conclusion : if  $n = s_1 s_2 \cdots s_t$ ,  $s_i \equiv 1 \pmod{4}$ , alors  $\frac{n-1}{4} \equiv \sum_{i=1}^t \frac{s_i-1}{4} \pmod{4}$ . □

**Ex. 9.45** Let  $\pi = a + bi \in \mathbb{Z}[i]$  and  $q \equiv 3 \pmod{4}$  a rational prime. Show  $\pi^q \equiv \bar{\pi} \pmod{4}$ .

*Proof.* Let  $\pi = a + bi \in \mathbb{Z}[i]$ , and  $q \equiv 3 \pmod{4}$  a rational prime.

As  $\binom{q}{k} \equiv 0 \pmod{q}$  for  $1 \leq k \leq q-1$ , the Fermat's Little Theorem gives

$$\begin{aligned} \pi^q &= (a + bi)^q \\ &\equiv a^q + b^q i^q \pmod{q} \\ &\equiv a + bi^3 \pmod{q} \\ &= a - bi \\ &= \bar{\pi} \end{aligned}$$

Conclusion :  $\pi^q \equiv \bar{\pi} \pmod{q}$  ( $\pi \in \mathbb{Z}[i]$ , and  $q \equiv 3 \pmod{4}$ ) □