Solutions to Ireland, Rosen "A Classical Introduction to Modern Number Theory"

Richard Ganaye

October 18, 2022

Chapter 9

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

Proof. Let $\lambda = 1 - \omega$, and $z = a + b\omega \in D = \mathbb{Z}[\omega], a, b \in \mathbb{Z}$.
 $\omega \equiv 1 \pmod{\lambda}$, so $z \equiv a + b \pmod{\lambda}$, with $c = a + b \in \mathbb{Z}$.
 $c \equiv 0, 1, -1 \pmod 3$, and since $\lambda \mid 3$, $z \equiv 0, 1, -1 \pmod{\lambda}$.
 Conclusion : every $z \in D$ is congruent to either $0, 1$, or -1 modulo $\lambda = 1 - \omega$.
 Note : $1 \not\equiv -1 \pmod{\lambda}$, 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 λ would be a unit, in contradiction with λ prime.
 So there exist exactly three classes modulo λ in $D : |D/\lambda D| = 3 = N(\lambda)$. $\qquad \square$

Ex. 9.2 *From now on we shall set $D = \mathbb{Z}[\omega]$ and $\lambda = 1 - \omega$. For μ 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 π_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 π be a prime in D. There are three cases.

- If $N(\pi) = 3$, then π is associate to $\lambda \in S$, and no associate of λ is primary.

- If $N(\pi) = q^2$, where $q \equiv -1 \pmod 3$ is a rational prime, then π 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 among the associates of π 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

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

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

Ex. 9.3 *Let γ 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 π 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).

$$N(\gamma) - 1 = (3m-1)^2 + (3n)^2 - 3n(3m-1) - 1$$
$$= 9m^2 - 6m + 9n^2 - 9nm + 3n$$
$$\frac{N(\gamma)-1}{3} = 3m^2 - 2m + 3n^2 - 3nm + n \equiv n + m \ [3]$$

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 ω^2 according to whether γ is congruent to 8,2, or 5 modulo 3λ. In particular, if q is a rational prime, $q \equiv 2 \pmod 3$, then $\chi_q(\omega) = 1, \omega$, or ω^2 according to whether $q \equiv 8, 2$, or 5 (mod 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

$$m + n\omega \equiv m + n \pmod \lambda$$
$$3(m + n\omega) \equiv 3(m + n) \pmod{3\lambda}$$
$$\gamma = -1 + 3(m + n\omega) \equiv -1 + 3(m + n) \pmod{3\lambda}$$

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

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

Conversely, if $\gamma \equiv 8 \equiv -1 \ [3\lambda]$, 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 $3 \mid m+n$, $m + n \equiv 0 \ [3]$, and so $\chi_\gamma(\omega) = 1$. The two other cases are similar, so we obtain

$$\chi_\gamma(\omega) = 1 \iff m + n \equiv 0 \ [3] \iff \gamma \equiv 8 \ [3\lambda],$$
$$\chi_\gamma(\omega) = \omega \iff m + n \equiv 1 \ [3] \iff \gamma \equiv 2 \ [3\lambda],$$
$$\chi_\gamma(\omega) = \omega^2 \iff m + n \equiv 2 \ [3] \iff \gamma \equiv 5 \ [3\lambda].$$

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

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

$$\chi_q(\omega) = 1 \iff q \equiv 8 \ [9],$$
$$\chi_q(\omega) = \omega \iff q \equiv 2 \ [9],$$
$$\chi_q(\omega) = \omega^2 \iff q \equiv 5 \ [9].$$

$\square$

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,

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

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

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

Conclusion :

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

$\square$

Ex. 9.6 *Prove that*

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

(b) $\chi_\gamma(\lambda) = \omega$ for $\gamma \equiv 5, 5 + 3\omega, 5 + 6\omega$ [9].

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

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

$$\chi_\gamma(\lambda) = 1 \iff m \equiv 0 \ [3] \Rightarrow \gamma \equiv 8 + 3n\omega \ [9] \Rightarrow \gamma \equiv 8, 8 + 3\omega, 8 + 6\omega \ [9]$$
$$\chi_\gamma(\lambda) = \omega \iff m \equiv 2 \ [3] \Rightarrow \gamma \equiv 5 + 3n\omega \ [9] \Rightarrow \gamma \equiv 5, 5 + 3\omega, 5 + 6\omega \ [9]$$
$$\chi_\gamma(\lambda) = \omega^2 \iff m \equiv 1 \ [3] \Rightarrow \gamma \equiv 2 + 3n\omega \ [9] \Rightarrow \gamma \equiv 2, 2 + 3\omega, 2 + 6\omega \ [9]$$

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.

$$\chi_\gamma(\lambda) = 1 \iff \gamma \equiv 8, 8 + 3\omega, 8 + 6\omega \ [9]$$
$$\chi_\gamma(\lambda) = \omega \iff \gamma \equiv 5, 5 + 3\omega, 5 + 6\omega \ [9]$$
$$\chi_\gamma(\lambda) = \omega^2 \iff \gamma \equiv 2, 2 + 3\omega, 2 + 6\omega \ [9]$$

$\square$

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.

$\square$

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.

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

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

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

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

Ex. 9.9 *Show that $\overline{\alpha} \neq 0$, the residue class of α, 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 π a prime in D, $N\pi \neq 3$, and $\alpha \in D, \pi \nmid \alpha$.
$\overline{\alpha}$ is a cube in $(D/\pi D)^*$
$\iff x^3 \equiv \alpha \pmod \pi$ has a solution in D
$\iff \chi_\pi(\alpha) = 1$ (by Prop. 9.3.3(a))
$\iff \alpha^{\frac{N\pi - 1}{3}} \equiv 1 \pmod \pi$
$\iff \overline{\alpha}^{\frac{N\pi - 1}{3}} = \overline{1}$.

The cubes in $(D/\pi D)^*$ are then the roots of the polynomial $f(x) = x^{\frac{N\pi - 1}{3}} - \overline{1}$ 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 8.1.1, 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 $\varphi : (D/\pi D)^* \to (D/\pi D)^*$ the group homomorphism defined by $\varphi(x) = x^3$.

Then $\text{im}(\varphi)$ is the set of cubes in $(D/\pi D)^*$.

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

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

Note : if $N\pi = 3$, that is to say, if π is associate to $1 - \omega$, $D/\pi D = \{\overline{0}, \overline{1}, \overline{2}\}$. As $\overline{1}^3 = \overline{1}, \overline{2}^3 = \overline{2}$, 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 $x^{24} - 1 = \displaystyle\prod_{\alpha \in (D/5D)^*} (x - \alpha)$.

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

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). $\qquad\square$

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 β in $D/5D$.)
To verify that $[\beta]$ has order 24, it is sufficient to verify that $[\beta]^8 \neq 1, [\beta]^{12} \neq 1$:
$\beta^8 = \omega^{16}\lambda^8 = \omega\lambda^8 = (\omega\lambda)^8\omega^2 \equiv \omega^2 \not\equiv 1 \pmod 5$.
$\beta^{12} = (\omega^2\lambda)^{12} = \lambda^{12} = (\omega\lambda)^{12} \equiv (\omega\lambda)^4 \equiv -1 \pmod 5$ (since $(\omega\lambda)$ has order 8 in $D/5D$).
Conclusion : $\omega\lambda$ has order 8, $\omega\lambda^2$ has order 24 in $(D/5D)^*$. $\qquad\square$

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

Proof. Let $\pi \in D, \overline{\pi} \neq 0$. Then $\overline{\pi}$ is a cube in $D/5D$ iff $\overline{\pi}^{(q^2-1)/3} = 1$, with $q = 5$, namely $\overline{\pi}^8 = 1$ (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 $\overline{\gamma}^k, 0 \le k \le 7$ are distinct roots of the polynomial $x^8 - 1$, which has at most 8 roots. Therefore the subgroup of cubes in $(D/5D)^*$ is

$$\{1, \overline{\gamma}, \overline{\gamma}^2, \ldots, \overline{\gamma}^7\}.$$

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

$$\gamma^0 = 1$$
$$\gamma^1 = 1 + 2\omega$$
$$\gamma^2 \equiv -3 \equiv 2 \ [5] \qquad \text{(Ex. 9.12)}$$
$$\gamma^3 = -3 - 6\omega \equiv 2 + 4\omega \ [5]$$
$$\gamma^4 \equiv -1 \equiv 4 \ [5]$$
$$\gamma^5 \equiv -1 - 2\omega \equiv 4 + 3\omega \ [5]$$
$$\gamma^6 \equiv 3 \ [5]$$
$$\gamma^7 \equiv 3 + 6\omega \equiv 3 + \omega \ [5]$$

Conclusion : If $\pi \not\equiv 0 \ (\mathrm{mod} \ 5)$, $\pi \equiv \alpha^3 \ (\mathrm{mod} \ 5), \alpha \in D$ iff

$$\pi \equiv 1, 2, 3, 4, 1 + 2\omega, 2 + 4\omega, 3 + \omega, 4 + 3\omega \ [5].$$

$\square$

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

Proof. If π is a primary prime, and not an associate of 5, the Law of Cubic Reciprocity gives

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

(see Ex. 9.13)

Conclusion : the equation $5 \equiv x^3 \ [\pi], x \in D$ is solvable iff the primary prime associate to π is congruent modulo 5 to $1, 2, 3, 4, 1 + 2\omega, 2 + 4\omega, 3 + \omega, 4 + 3\omega$.

Examples :

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

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

Indeed , $7^3 \equiv 5^3 \equiv 11^3 \equiv 5 \ (\mathrm{mod} \ 13)$, and $3 - \omega \mid 13$, so $7^3 \equiv 5^3 \equiv 11^3 \equiv 5$ (mod $3 - \omega$). $\square$

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

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

Conversely, suppose that $\chi_\pi(a) = 1$. Then the equation $y^3 \equiv a \ (\mathrm{mod} \ \pi)$ 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 π (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 π is 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 $\mathbb{Z}$. $\qquad\square$

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 $x^3 = 11 \pmod 7$ 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,

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

Moreover, by Proposition 7.1.2,

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

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 $\omega^2 x = 7 - \omega, \omega x = -8 - 7\omega \equiv 3 + 4\omega \pmod{11}$) :

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

$\hfill\square$

Ex. 9.17 *An element $\gamma \in D$ is called primary if $\gamma \equiv 2 \pmod 3$. If γ and ρ are primary, show that $-\gamma\rho$ is primary. If γ is primary, show that $\gamma = \pm\gamma_1\gamma_2 \ldots \gamma_t$, where the γ_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, γ can be written

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

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

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

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

where the γ_i are primary primes. $\qquad \square$

Ex. 9.18 *(continuation) If $\gamma = \pm \gamma_1 \gamma_2 \cdots \gamma_t$ is a primary decomposition of the primary element γ, define $\chi_\gamma(\alpha) = \chi_{\gamma_1}(\alpha) \chi_{\gamma_2}(\alpha) \cdots \chi_{\gamma_t}(\alpha)$. 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 ρ is primary, show that $\chi_\rho(\alpha)\chi_\gamma(\alpha) = \chi_{-\rho\gamma}(\alpha)$.*

Proof. If $\alpha \equiv \beta \ [\gamma]$, 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,

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

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

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

$\qquad \square$

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

$$-\gamma_1 \gamma_2 = -A_1 A_2 + B_1 B_2 + (-A_1 B_2 - A_2 B_1 + B_1 B_2)\omega = A + B\omega,$$

therefore

$$3M - 1 = A = -A_1 A_2 + B_1 B_2 \equiv 3(M_1 + M_2) - 1 \pmod 9,$$

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

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

$\square$

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

Proof. ρ, γ 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 ρ_i, γ_i are primary primes. By the law of Cubic Reciprocity, we obtain

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

$\square$

Ex. 9.21 *If γ is primary, show that there are infinitely many primary primes π such that $x^3 \equiv \gamma \pmod{\pi}$ is not solvable. Show also that there are infinitely many primary primes π 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 γ is not the cube of some element of D (in the contrary case $x^3 \equiv \gamma \pmod{\pi}$ is solvable for all prime π).

Note first that for all primes π 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 $\overline{\tau} \in (D/\pi D)^*$ 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 γ is primary. Then $\gamma = \pm \gamma_1^{n_1} \gamma_2^{n_2} \cdots \gamma_p^{n_p}$, where the γ_i are distinct primary primes. Write $n_i = 3q_i + r_i$, $r_i \in \{0, 1, 2\}$. Then grouping in γ' the γ^{r_i} such that $r_i \neq 0$, we can write $\gamma = \delta^3 \gamma'$, $\gamma' = \gamma_1^{r_1} \gamma_2^{r_2} \cdots \gamma_l^{r_l}$, $r_i \in \{1, 2\}$, $\delta = \pm \gamma_1^{q_1} \cdots \gamma_p^{n_p} \in D$ (-1 is a cube). Since by hypothesis γ 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 γ_i are not associate to $\lambda = 1 - \omega$ (see Ex. 9.17).

Let $A = \{\lambda_1, \lambda_2, \ldots, \lambda_k\}$ a set (possibly empty) of distinct primary primes λ_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 λ_{k+1} distinct of the λ_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 π 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 $3 = \lambda \overline{\lambda} = -\omega^2 \lambda^2$ is relatively prime to γ_i, λ_i, there exists $\beta \in D$ such that

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

The first equation show that β is primary, so $\beta = (-1)^{m-1} \beta_1 \ldots \beta_m$, where the β_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 ρ, γ, 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 $\beta \not\equiv 0$ $[\gamma_i]$, β_j is distinct of the λ_i and γ_i, and β_j is not associate to λ 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 λ_{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 π.

To initialize the induction, we display such a prime π, namely $\pi = 2 + 3\omega$. Indeed, $N(\pi) = 4 + 9 - 6 = 7$, 7 is a rational prime, so π 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 π is not associate to $\lambda = 1 - \omega$.

Suppose now the existence of a set $A = \{\lambda_1, \lambda_2, \ldots, \lambda_l\}, l \geq 1$, of distinct primary primes λ_i, not associate to λ 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 λ_{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 β_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 $\beta = 3(-1)^{l-1}\lambda_1 \cdots \lambda_l - 1$, β_i is associate neither to λ_i nor to λ. 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 π.

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

To initialize the induction, we display such a prime π, namely $\pi = -4 + 3\omega$. Indeed, $N(\pi) = 16 + 9 + 12 = 37$, 37 is a rational prime, so π 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 $A = \{\lambda_1, \lambda_2, \ldots, \lambda_l\}, l \geq 1$, of distinct primary primes λ_i, not associate to λ and such the equation $x^3 \equiv \lambda$ $[\lambda_i]$ is not solvable. We will show that we can add a prime λ_{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 β_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 $\beta = 3(-1)^{l-1}\lambda_1 \cdots \lambda_l - 1$, β_i is associate neither to λ_i nor to λ. 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 π.

$\square$

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 finitely many primary primes π, then γ is a cube in D.*

Proof. Let $\gamma \in D$ and suppose that γ 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 γ_i are distinct primary primes, not associate to λ. 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

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

without cubic factors.

- Case 1 : $l \geq 1$.

  Let $A = \{\lambda_1, \ldots, \lambda_k\}$ a possibly empty set of distinct primary primes λ_i, distinct of the γ_i, not associate to λ, and such that the equation $x^3 \equiv \gamma \ [\lambda_i]$ is not solvable. We will show that we can add a prime λ_{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 $\beta \equiv -1 \ [3]$: β 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,

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

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

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

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

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

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

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

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

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

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

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

$\beta \equiv 2$ [3] : β 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

$$\chi_\beta(\omega) = \omega^{M+N} = \omega^{9m-2+9n-1} = 1$$
$$\chi_\beta(\lambda) = \omega^{2M} = \omega^{2(9m-2)} = \omega^2 \ne 1$$

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

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

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

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 π_0 is relatively prime to λ, 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 π such that $x^3 \equiv \gamma \ [\pi]$ is not solvable.

• Conclusion :

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

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

$\square$

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 $p = \pi\overline{\pi}$, 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 $p \equiv 1 \pmod 3$, $D/\pi D = \{\overline{0}, \ldots, \overline{p-1}\}$, 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 $p \equiv 1 \pmod 3$.

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

$\square$

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

Proof. By hypothesis, π is a primary prime, so $\pi = 3m - 1 + 3n\pi$, $m, n \in \mathbb{Z}$.

(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 π, 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

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

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 π primary prime in D (and also $\bar\pi$), and by definition of χ_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)), so $\chi_p(b) = 1$. a has a decomposition in prime factors of the form :

$$a = \pm q_1 q_2 \cdots q_k p_1 p_2 \cdots p_l = \pm q_1 q_2 \cdots q_k \pi_1 \overline{\pi_1} \pi_2 \overline{\pi_2} \cdots \pi_l \overline{\pi_l},$$

where $q_i \equiv -1, p_j \equiv 1 \pmod 3$, and the π_k are primary primes (since all these elements are primary, the symbol $\pm$ is $(-1)^{k-1}$). Thus, by Ex. 9.21,

$$\chi_a(b) = \chi_{q_1}(b) \cdots \chi_{q_k(b)} \chi_{\pi_1}(b) \chi_{\overline{\pi_1}}(b) \cdots \chi_{\pi_l}(b) \chi_{\overline{\pi_l}}(b) = 1.$$

(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 implies $r = p$. But then $p \mid \pi, N(p) \mid N(\pi), p^2 \mid p$: this is absurd. As a is relatively prime to b in $\mathbb{Z}$, $ua + vb = 1$, $u, v \in \mathbb{Z}$, so a, b are relatively prime in D, each prime factor $q_i, \pi_i, \overline{\pi_i}$ of b is relatively prime to a.)

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

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

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

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

$\square$

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 χ_{a+b} has order 3,

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

$\chi_{a+b}(3) = 1$ car $(a + b) \wedge 3 = (3(m + n) - 1) \wedge 3 = 1$.
$\chi_{a+b}(\omega) = \omega^{m+n}$ (Ex. 9.19).
Conclusion :
$$\chi_{a+b}(1 - \omega) = \omega^{2(m+n)}.$$

$\square$

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

Proof. π and $a + b$ are primary elements of D, so

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

By Exercises 9.24 and 9.25,

$$\begin{aligned}
\chi_\pi(a + b) &= \omega^{2n}\chi_\pi(1 - \omega) \\
\chi_{a+b}(\pi) &= \omega^{2(m+n)}
\end{aligned}$$

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

$\square$

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 an older edition.)

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

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

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

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

(a)   • Case 1 : $a \equiv 1 \ [4], b \equiv 0[4]$. 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 $a \equiv 1[4]$, thus $a \equiv (-1)^{(p-1)/4} \ [4]$.

   • Case 2 : $a \equiv 3 \ [4], b \equiv 2 \pmod 4$.
$a = 4A+3, b = 4B+2, a^2+b^2-1 = 16A^2+24A+9+16B^2+16B+4-1 \equiv 4 \ [8]$,
so $(a^2+b^2-1)/4 \equiv 1 \ [2], (-1)^{(p-1)/4} = (-1)^{(a^2+b^2-1)/4} = -1$, and $a \equiv -1 \ [4]$,
thus $a \equiv (-1)^{(p-1)/4} \ [4]$.

In both cases,

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

(b) In every case, $b \equiv a - 1 \ [4]$, thus

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

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

$$p \equiv 1 \ [8] \iff \pi \equiv 1 \ [4],$$
$$p \equiv 5 \ [8] \iff \pi \equiv 3 + 2i \ [4].$$

$\square$

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

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

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

$\square$

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 an 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 an unit.

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

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

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 8.9.6 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

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

$\square$

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

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

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

If $a \equiv 1 \pmod 4$, then $(-1)^{(a-1)/2} = 1$.
If $a \equiv 3 \pmod 4$, then $b \equiv 2$ [4] :

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

so $(p+3)/4 \equiv 0$ [2].
In both cases $(-1)^{((a-1)/2)\,((p+3)/4)} = 1$, and so

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

$\square$

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 a prime, $p \equiv 1$ [4], then $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1$ [p].
  By Wilson's theorem (Prop. 4.1.1, Corollary), $(p-1)! \equiv -1$ [p].

$$-1 \equiv (p-1)! = 1.2. \cdots . \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) \cdots (p-2)(p-1)$$

$$\equiv 1.2. \cdots \frac{p-1}{2}\left[-\left(\frac{p-1}{2}\right)\right]\cdots(-2)(-1)$$

$$\equiv (-1)^{(p-1)/2}\left[\left(\frac{p-1}{2}\right)!\right]^2$$

$$\equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \ [p],$$

since $p \equiv 1$ [4].

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

  By lemma 5 section 7, as $p \equiv 1$ [4], there exists an irreducible π such that $N(\pi) = p$, and we can choose π 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 $p = a^2 + b^2, a \equiv 1$ [4]$, b \equiv -((p-1)/2)! \, a$ [p].

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

  $$p = a^2 + b^2, a \equiv 1 \ [4], b \equiv -((p-1)/2)! \, a \ [p].$$

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

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

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

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

  $p = a^2 + b^2 = a^2 + d^2$, so $d = \pm b$, and $d \equiv b$ [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 $p \equiv 1$ [4], there exists an unique pair a, b such that

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

$\square$

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.

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

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

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

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

$\qquad\square$

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

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

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

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

$\square$

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 $\equiv 1$
(mod 4) and use Proposition 9.9.8. Note $a + b \equiv 1$ (mod 4).]

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

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

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

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

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

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

If $n > 0$, $n = q_1 q_2 \cdots q_k p_1 p_2 \cdots p_l$, where $q_i \equiv -1 \ [4], p_i \equiv 1 \ [4]$, 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

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

where $s_i \equiv 1 \ [4], \ 1 \leq i \leq N$.

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

the last equality resulting of Exercise 9.44.

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

Let $\pi = a + bi, a \wedge b = 1$ a primary irreducible. As $a(1+i) = a + b + i(a+bi)$, $a(1+i) \equiv a + b \ [\pi]$, so
$$\chi_\pi(a)\chi_\pi(1+i) = \chi_\pi(a+b).$$

As $\pi = a + bi$ is primary, $a + b \equiv 1 \ [4]$.

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

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

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

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

$a + b \equiv 1 \ [4]$, 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

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

$\square$

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 π 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 $q \equiv 3$ (mod 4).

If $u = \pm i$, then $\pi = \pm q = a + bi$ is such that b is odd, in contradiction with π primary. Thus $u = \pm 1$, and $\pi = \varepsilon q, \varepsilon = \pm 1$. As π 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 $\pi \equiv 1 \ [4], \chi_\pi(a) = i^{(a-1)/2}$,

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

$\square$

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 $q \equiv 3$ (mod 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

$$\frac{q^2 - 1}{4} = 4k^2 + 2k$$

$$\equiv 2k = \frac{a-1}{2} \quad \text{(mod 4)}.$$

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 π.

$\square$

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 π 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),

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

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

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

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

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],
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 $p \equiv 1$ [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 π is primry, $a \equiv b+1 \equiv -b+1 \pmod 4$, therefore

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

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 π 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 $0, 1, \cdots, p-1$, 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 $p \equiv 1 \pmod 4$, $p = \pi\overline{\pi}$, 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 :

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

$\square$

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

Proposition 9.8.3(d) *If π 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, $a \equiv 1 \ [4], b \equiv 0 \ [4]$, or $a \equiv 3[4], b \equiv 2[4]$.

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

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

- If $a \equiv 3 \ [4], b \equiv 2 \ [4]$, 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 π is a primary irreducible in $\mathbb{Z}[i]$, then

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

$\square$

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 a rational prime, $p \equiv 1 \pmod 6$. As $p \equiv 1 \pmod 3$, $p = N(\pi)$, where $\pi = a + b\omega$ is a primary prime. $p = N(\pi) = a^2 - ab + b^2, 4p = (2a-b)^2 + 3b^2$. As π is primary, $a \equiv 2 \pmod 3, b \equiv 0 \pmod 3$, so $4p = A^2 + 27B^2$, with $A = 2a - b \equiv 1 \pmod 3, b = B/3$.

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

$$2 \mid B \iff 2 \mid b \iff (b \equiv 0\ [2], a \equiv 1\ [2]) \iff \pi \equiv 1\ [2].$$

By Proposition 9.6.1, $2 \mid B$ iff $\pi \equiv 1\ [2]$, iff $x^3 - 2$ is solvable in D, iff $\chi_\pi(2) = 1$.
By Exercise 8.6,

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

where ρ is the Legendre's character.
Here $\chi_\pi(2) = 1$, so $J(\chi_\pi, \chi_\pi) = J(\chi_\pi, \rho)$, and by Lemma 1 section 4,

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

By Exercise 8.15,
$$N(y^2 = x^3 + 1) = p + A,$$

and the Exercise 8.27(b) gives

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

and by Exercise 8.27(c),

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

where $m = (p-1)/6$. Therefore

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

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

where $\chi_\pi(2)^{-2} = \chi_\pi(2) \in \{1, \omega, \omega^2\}$.
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 $-b\omega \equiv \pm b \pmod \pi$. As $\pi \nmid b$, $\pi \mid \omega \pm 1$, with π primary : it's impossible ($\omega + 1$ is a unit and $\omega - 1$ is prime).

If $\chi_\pi(2) = \omega^2$, then $a + b\omega = \omega^2(c + d\omega), a + b\omega^2 = \omega(c + d\omega^2)$: same contradiction.

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

Conclusion :

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

$\square$

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

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

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

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

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

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

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

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

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

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

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

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

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