

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

Richard Ganaye

August 30, 2023

Chapter 7

Ex. 7.1 Use the method of Theorem 1 to show that a finite subgroup of the multiplicative group of a field is cyclic.

A solution is already given in Ex. 4.15

Ex. 7.2 Find the finite subgroups of \mathbb{R}^* and \mathbb{C}^* and show directly that they are cyclic.

Proof. If G is a finite subgroup of \mathbb{R} or \mathbb{C} , and $n = |G|$, then from Lagrange’s Theorem, $x^n = 1$ for all $x \in G$.

- If G is a finite subgroup of \mathbb{R}^* , then the solutions of $x^n = 1$ are in $\{-1, 1\}$, so $\{1\} \subset G \subset \{-1, 1\}$: $G = \{1\}$ or $G = \{-1, 1\}$, both cyclic.

- If G is a finite subgroup of \mathbb{C}^* , then $G \subset \mathbb{U}_n = \{e^{2ik\pi/n} \mid 0 \leq k \leq n-1\}$. As $|G| = |\mathbb{U}_n| = n$, then $G = \mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$ is cyclic. \square

Ex. 7.3 Let F a field with q elements and suppose that $q \equiv 1 \pmod{n}$. Show that for $\alpha \in F^*$, the equation $x^n = \alpha$ has either no solutions or n solutions.

Proof. This is a particular case of Prop. 7.1.2., where $d = n \wedge (q-1) = n$: the equation $x^n = \alpha$ has solutions iff $\alpha^{(q-1)/n} = 1$. In this case, there are exactly $d = n$ solutions.

We give here a direct proof.

Let g be a generator of F^* . Write $x = g^y, \alpha = g^a$. Then

$$x^n = \alpha \iff g^{ny} = g^a \iff q-1 \mid ny - a.$$

Suppose that there exists $x \in F$ such that $x^n = \alpha$. Then there exists $y \in \mathbb{Z}$ such that $q-1 \mid ny - a$. Since $n \mid q-1$, then $n \mid a$.

$$q-1 \mid ny - a \iff \frac{q-1}{n} \mid y - \frac{a}{n} \iff y = \frac{a}{n} + k \frac{q-1}{n}, k \in \mathbb{Z}.$$

As $\frac{a}{n} + (k+n) \frac{q-1}{n} = \frac{a}{n} + k \frac{q-1}{n}, k \in \mathbb{Z}$, the values $k = 0, 1, \dots, n-1$ are sufficient :

$$x^n = \alpha \iff y = \frac{a}{n} + k \frac{q-1}{n}, k \in \{0, 1, \dots, n-1\}.$$

Moreover, these solutions are all distinct : if $k, l \in \{0, 1, \dots, n-1\}$,

$$\begin{aligned} g^{\frac{a}{n} + k \frac{q-1}{n}} &= g^{\frac{a}{n} + l \frac{q-1}{n}} \Rightarrow g^{(k-l) \frac{q-1}{n}} = 1 \\ &\Rightarrow q-1 \mid (k-l) \frac{q-1}{n} \\ &\Rightarrow n \mid k-l \\ &\Rightarrow k \equiv l \pmod{n} \Rightarrow k = l. \end{aligned}$$

Conclusion: if F is a field with q elements and $n \mid q-1$, the equation $x^n = \alpha$ has either no solutions or n solutions in F .

Note:

$$\exists x \in F^*, x^n = \alpha \iff n \mid a \iff \alpha^{(q-1)/n} = 1.$$

Indeed, if $x^n = \alpha$ has a solution, we have proved that $n \mid a$, thus $\alpha^{(q-1)/n} = (g^{a/n})^{q-1} = 1$.

Conversely, if $\alpha^{(q-1)/n} = 1$, $g^{a(q-1)/n} = 1$, thus $q-1 \mid a(q-1)/n$, so $n \mid a$: $\alpha = x^n$, with $x = g^{a/n}$. \square

Ex. 7.4 (continuation) Show that the set of $\alpha \in F^*$ such that $x^n = \alpha$ is solvable is a subgroup with $(q-1)/n$ elements.

Proof. Here $n \mid q-1$.

Let $\varphi = F^* \rightarrow F^*$ be the application defined by $\varphi(x) = x^n$. Then φ is a homomorphism of groups, and $\ker \varphi$ is the set of solutions of $x^n = 1$. As $n \mid q-1$, $x^n = 1$ has exactly n solutions (Prop 7.1.1, Corollary2, or Ex 7.3 with $\alpha = 1$). So $|\ker \varphi| = n$.

Thus $\text{Im } \varphi \simeq F^*/\ker \varphi$ is a subgroup with cardinality $|F^*|/|\ker \varphi| = (q-1)/n$, and $\text{Im } \varphi$ is the set of α such that $x^n = \alpha$ is solvable.

Conclusion: the set of $\alpha \in F^*$ such that $x^n = \alpha$ is solvable is a subgroup with $(q-1)/n$ elements. \square

Ex. 7.5 (continuation) Let K be a field containing F such that $[K : F] = n$. For all $\alpha \in F^*$, show that the equation $x^n = \alpha$ has n solutions in K . [Hint: Show that $q^n - 1$ is divisible by $n(q-1)$ and use the fact that $\alpha^{q-1} = 1$.]

Proof. As $q \equiv 1 \pmod{n}$, $\frac{q^n-1}{q-1} = 1 + q + \dots + q^{n-1} \equiv 0 \pmod{n}$, then $n \mid \frac{q^n-1}{q-1}$:

$$q^n - 1 = kn(q-1), k \in \mathbb{N}.$$

Since $\alpha \in F^*$, $\alpha^{q-1} = 1$, thus

$$\alpha^{(q^n-1)/n} = (\alpha^{q-1})^k = 1.$$

As $|K| = q^n$, Prop. 7.1.2 (or the final remark in Ex.7.3) show that there exists $x \in K^*$ such that $x^n = \alpha$. Then, from Ex.7.3, we know that there exist n solutions in K .

Conclusion: if $[K : F] = n$, for all $\alpha \in F^*$, the equation $x^n = \alpha$ has n solutions in K . \square

Ex. 7.6 Let $K \supset F$ be finite fields with $[K : F] = 3$. Show that if $\alpha \in F$ is not a square in F , it is not a square in K .

Proof. Let $q = |F|$. Then $|K| = q^3$.

If the characteristic of F is 2, then $q = 2^k$ for some integer $k \geq 1$, and for all $x \in F$, $x = x^q = \left(x^{2^{k-1}}\right)^2$. Therefore all elements in F (or K) are squares. We can now suppose that the characteristic of F is not 2, so that $1 \neq -1$ in F .

As α is not a square in F , $\alpha^{(q-1)/2} \neq 1$ (Prop. 7.1.2). From $0 = \alpha^{q-1} - 1 = (\alpha^{(q-1)/2} - 1)(\alpha^{(q-1)/2} + 1)$, we deduce that $\alpha^{(q-1)/2} = -1$. Then

$$\alpha^{(q^3-1)/2} = (\alpha^{(q-1)/2})^{q^2+q+1} = (-1)^{q^2+q+1} = -1,$$

since $q^2 + q + 1$ is always odd.

$\alpha^{(q^3-1)/2} \neq 1$: this implies (Prop. 7.1.2) that α is not a square in K . \square

Ex. 7.7 Generalize Exercise 6 by showing that if α is not a square in F , it is not a square in any extension of odd degree and is a square in every extension of even degree.

Proof. Write $n = [K : F]$, and $q = \text{Card } F$.

As α is not a square in F , the characteristic of F is not 2 (see Ex.7.6), and $\alpha^{(q-1)/2} \neq 1$. Since $\alpha^{q-1} = 1$, $\alpha^{(q-1)/2} = -1$.

$$\alpha^{(q^n-1)/2} = (\alpha^{(q-1)/2})^{1+q+\dots+q^{n-1}} = (-1)^{1+q+\dots+q^{n-1}}.$$

• If n is odd, $1+q+\dots+q^{n-1} \equiv 1 \pmod{2}$, thus $\alpha^{(q^n-1)/2} = -1 \neq 1$, and consequently α is not a square in K .

• If n is even, as q is odd ($\text{char}(F) \neq 2$), $1+q+\dots+q^{n-1} \equiv 0 \pmod{2}$, thus $\alpha^{(q^n-1)/2} = 1$, so α is a square in K . \square

Ex. 7.8 In a field with 2^n elements, what is the subgroup of squares.

Let F be a field with $q = 2^n$ elements.

Proof 1

Proof. $d = (q-1) \wedge 2 = (2^n-1) \wedge 2 = 1$, thus each $\alpha \in F^*$ verifies $\alpha^{(q-1)/d} = \alpha^{q-1} = 1$. Theorem 7.1.2 show that α is a square in F , of exactly one root.

The subgroup of squares is F^* . \square

Proof 2

Proof. For all $x \in F$, $x = x^q = \left(x^{2^{n-1}}\right)^2$. So all elements in F are squares. \square

Ex. 7.9 If $K \supset F$ are finite fields, $|F| = q$, $\alpha \in F$, $q \equiv 1 \pmod{n}$, and $x^n = \alpha$ is not solvable in F , show that $x^n = \alpha$ is not solvable in K if $(n, [K : F]) = 1$.

Proof. Let $k = [K : F]$. From hypothesis, $k \wedge n = 1$, so there exist integers u, v such that $uk + vn = 1$.

As $n \mid q-1$, $n \wedge (q-1) = n$, the hypothesis " $x^n = \alpha$ is not solvable in F " implies that $\alpha^{(q-1)/n} \neq 1$ (Prop. 7.1.2).

Write $\omega = \alpha^{(q-1)/n}$, so $\omega \neq 1$ and $\omega^n = 1$.

As $n \mid q - 1$, $n \mid q^k - 1$ and

$$\alpha^{(q^k-1)/n} = (\alpha^{(q-1)/n})^{1+q+q^2+\dots+q^{k-1}} = \omega^{1+q+q^2+\dots+q^{k-1}}.$$

Moreover $1 + q + \dots + q^{k-1} \equiv k \pmod{n}$, and $\omega^n = 1$, so $\alpha^{(q^k-1)/n} = \omega^k$.

If $\omega^k = 1$, then $\omega = \omega^{uk+vn} = (\omega^k)^u(\omega^n)^v = 1$, which is in contradiction with $\omega = \alpha^{(q-1)/n} \neq 1$.

Thus $\alpha^{(q^k-1)/n} = \omega^k \neq 1$. This proves that the equation $x^n = \alpha$ has no solution in K . \square

Ex. 7.10 If $K \supset F$ be finite fields and $[K : F] = 2$. For $\beta \in K$, show that $\beta^{1+q} \in F$ and moreover that every element in F is of the form β^{1+q} for some $\beta \in K$.

Proof. If $\beta = 0$, $\beta^{1+q} = 0 \in F$, and if $\beta \in K^*$, $\beta^{q^2-1} = 1$, so $(\beta^{1+q})^{q-1} = 1$, thus $\beta^{1+q} \in F$ (Prop. 7.1.1, Corollary 1).

Let g be a generator of K^* . Then $K^* = \{1, g, g^2, \dots, g^{q^2-2}\}$.

For every integer $k \in \mathbb{Z}$,

$$g^k \in F^* \iff (g^k)^{q-1} = 1 \iff g^{k(q-1)} = 1 \iff q^2 - 1 \mid k(q-1) \iff q+1 \mid k.$$

Thus $F^* = \{1, g^{q+1}, g^{2(q+1)}, \dots, g^{(q-2)(q+1)}\}$. If $\alpha \in F^*$, there exists $i, 0 \leq i \leq q-1$, such that $\alpha = g^{i(q+1)}$. If we write $\beta = g^i$, then $\alpha = \beta^{1+q}$ (and for $\alpha = 0$, we take $\beta = 0$).

Conclusion: if K is a quadratic extension of F (F, K finite fields), every element in F is of the form β^{1+q} for some $\beta \in K$. \square

Ex. 7.11 With the situation being that of Exercise 10 suppose that $\alpha \in F$ has order $q-1$. Show that there is a $\beta \in K$ with order q^2-1 such that $\beta^{1+q} = \alpha$.

Write $|a|$ the order of an element a in a group G . We recall the following lemma :

Lemma. If $|a| = d$, then for all $i \in \mathbb{Z}$, $|a^i| = \frac{d}{d \wedge i}$.

Proof. Indeed, for all $k \in \mathbb{Z}$,

$$(a^i)^k = e \iff a^{ik} = e \iff d \mid ik \iff \frac{d}{d \wedge i} \mid \frac{i}{d \wedge i} k \iff \frac{d}{d \wedge i} \mid k.$$

\square

Proof. (Ex. 7.11)

Let $\alpha \in F^*$ with $|\alpha| = q-1$, and g a generator of K^* , so $|g| = q^2-1$. We know from exercise 7.10 that there exists an integer i such that $\alpha = g^{i(q+1)}$.

Let $h = g^{q+1}$. As $h^{q-1} = 1$, then $h \in F^*$, and since $|g| = q^2-1$, $|h| = q-1$, so h is a generator of F^* .

Note that for all $s \in \mathbb{Z}$, $\alpha = g^{(i+s(q-1))(q+1)}$, since $g^{q^2-1} = 1$.

We will show that we can choose s such that $j = i + s(q-1)$ is relatively prime with $q+1$. Then j is such that $\alpha = g^{j(q+1)} = h^j$.

i is odd : if not, α is an element of the subgroup of squares in F^* , so its order divides $(q-1)/2$, in contradiction with $|\alpha| = q-1$.

$(q-1) \wedge (q+1) \mid 2$. Since $i-1$ is even, there exist integers s, t verifying the Bézout's equation

$$i-1 = t(q+1) - s(q-1).$$

Then $j = i + s(q - 1) = 1 + t(q + 1)$ is relatively prime with $q + 1 : j \wedge (q + 1) = 1$.

Moreover, as $\alpha = h^j$, with $|\alpha| = |h| = q - 1$, the lemma implies that

$$q - 1 = |\alpha| = \frac{q - 1}{(q - 1) \wedge j},$$

so $(q - 1) \wedge j = 1$. As $(q + 1) \wedge j = 1$ and $(q - 1) \wedge j = 1$, then $(q^2 - 1) \wedge j = 1$.

Let $\beta = g^j$. Then $\alpha = \beta^{1+q}$, and using the lemma,

$$|\beta| = |g^j| = \frac{q^2 - 1}{(q^2 - 1) \wedge j} = q^2 - 1.$$

Conclusion: there exists a $\beta \in K^*$ with order $q^2 - 1$ such that $\beta^{1+q} = \alpha$. \square

Ex. 7.12 Use Proposition 7.2.1 to show that given a field k and a polynomial $f(x) \in k[x]$ there is a field $K \supset k$ such that $[K : k]$ is finite and $f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ in $K[x]$.

Proof. We show by induction on the degree n of f that for all polynomials $f \in k[x]$ with $\deg(f) = n \geq 1$, there exists a field extension K such that $[K : k]$ is finite, and $f(x)$ splits in linear factors on K .

If $n = 1$, $f(x) = ax + b = a(x - \alpha_0)$, where $\alpha_0 = -b/a : K = k$ is suitable.

Suppose that the property is true for all polynomials of degree less than n on an arbitrary field k .

Let $f(x) \in k[x]$, $\deg(f) = n$. From proposition 7.2.1. applied to an irreducible factor of f , there exists a field L , $[L : K] < \infty$ and $\alpha \in L$ such that $f(\alpha_1) = 0$. Then $f(x) = (x - \alpha_1)g(x)$, $g(x) \in L[x]$.

Applying the induction hypothesis in the field L on the polynomial $g \in L[x]$ with $\deg(g) = n - 1$, we obtain a field K , $[K : L] < \infty$ such that $g(x) = a(x - \alpha_2) \cdots (x - \alpha_n)$ with $\alpha_i \in K$. So $f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ splits in linear factors in K . The induction is done. \square

Ex. 7.13 Apply Exercise 7.12 to $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and $f(x) = x^{p^n} - x$ to obtain another proof of Theorem 2.

Proof. Let $f(x) = x^{p^n} - x$. We know from Ex. 7.12 that there exists a finite extension K of \mathbb{F}_p such that f splits in linear factors on K :

$$f(x) = \prod_{k=1}^{p^n} (x - \alpha_k), \quad \alpha_1, \dots, \alpha_{p^n} \in K.$$

The set $k = \{\alpha_1, \dots, \alpha_{p^n}\} \subset K$ of the roots of $x^{p^n} - x$ is a subfield of K . Indeed, if $\alpha, \beta \in k$,

- (a) $f(1) = 0$, so $1 \in k$
- (b) $(\alpha - \beta)^{p^n} = \alpha^{p^n} - \beta^{p^n} = \alpha - \beta$, so $\alpha - \beta \in k$.
- (c) $(\alpha\beta)^{p^n} = \alpha^{p^n} \beta^{p^n} = \alpha\beta$, so $\alpha\beta \in k$.
- (d) $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$, so $\alpha^{-1} \in k$ if $\alpha \neq 0$.

As $f'(x) = -1$, $f(x) \wedge f'(x) = 1$. Thus f has no multiple root, and the cardinality of k is p^n .

Let $g(x) \in \mathbb{F}_p[x]$ a factor of $f(x)$, irreducible in $\mathbb{F}_p[x]$, with $d = \deg(g)$. As $g \mid f$, g splits in linear factors in $k[x]$. Let α be a root of $g(x)$ in k . As g is irreducible on \mathbb{F}_p , $d = \deg(g) = [\mathbb{F}_p[\alpha] : \mathbb{F}_p]$. Moreover $n = [k : \mathbb{F}_p] = [k : \mathbb{F}_p[\alpha]] [\mathbb{F}_p[\alpha] : \mathbb{F}_p]$, so $d \mid n$.

Conversely, suppose that g is any irreducible polynomial in $\mathbb{F}_p[x]$, with $d = \deg(g) \mid n$. Then $K_0 = \mathbb{F}_p[x]/\langle g \rangle$ contains a root α of g , and $[K_0 : \mathbb{F}_p] = \deg(g) = d$, so $\alpha^{p^d} = \alpha$.

As $d \mid n$, then $p^d - 1 \mid p^n - 1$ and $x^{p^d-1} - 1 \mid x^{p^n-1} - 1$ (Lemma 2,3 in section 1), thus

$$x^{p^d} - x \mid x^{p^n} - x.$$

$f(\alpha) = \alpha^{p^n} - \alpha = 0$ and g is the minimal polynomial of α , so $g \mid f$.

Since f has no multiple roots in K , $g^2 \nmid f$.

Conclusion :

$$x^{p^n} - x = \prod_{d \mid n} F_d(x),$$

where $F_d(x)$ is the product of the monic irreducible polynomial of degree d . \square

Ex. 7.14 Let F be a field with q elements and n a positive integer. Show that there exist irreducible polynomials in $F[x]$ of degree n .

Proof. Let $F = \mathbb{F}_q$ a field with $q = p^m$ elements, and n a positive integer.

By Theorem 2 Corollary 3, there exists an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree nm . Let g be an irreducible factor of f in $\mathbb{F}_q[x]$, and let α be a root of g in an extension of \mathbb{F}_q .

We show that $\mathbb{F}_q \subset \mathbb{F}_p[\alpha]$.

\mathbb{F}_q and $\mathbb{F}_p[\alpha]$ are two subfields of the same finite field $\mathbb{F}_q[\alpha]$. Moreover, $|\mathbb{F}_q| = p^m$, and $|\mathbb{F}_p[\alpha]| = p^{nm}$. As $m \mid nm$, $\mathbb{F}_q \subset \mathbb{F}_p[\alpha]$.

Indeed, for all $\gamma \in \mathbb{F}_q[\alpha]$,

$$\gamma \in \mathbb{F}_q \Rightarrow \gamma^{p^m} = \gamma \Rightarrow \gamma^{p^{mn}} = \gamma \Rightarrow \gamma \in \mathbb{F}_p[\alpha].$$

So $\mathbb{F}_q \subset \mathbb{F}_p[\alpha]$.

We show that $\mathbb{F}_q[\alpha] = \mathbb{F}_p[\alpha]$.

As $\mathbb{F}_p \subset \mathbb{F}_q$, $\mathbb{F}_p[\alpha] \subset \mathbb{F}_q[\alpha]$.

Let $\beta \in \mathbb{F}_q[\alpha]$. Then $\beta = \sum_{i=1}^k a_i \alpha^i$, where $a_i \in \mathbb{F}_q \subset \mathbb{F}_p[\alpha]$, thus $a_i = p_i(\alpha)$, $p_i \in \mathbb{F}_p[x]$.

Therefore

$$\beta = \sum_{i=1}^k p_i(\alpha) \alpha^i \in \mathbb{F}_p[\alpha].$$

We have proved $\mathbb{F}_q[\alpha] = \mathbb{F}_p[\alpha]$.

Since $|\mathbb{F}_p[\alpha]| = p^{nm}$,

$$nm = [\mathbb{F}_p[\alpha] : \mathbb{F}_p] = [\mathbb{F}_q[\alpha] : \mathbb{F}_p] = [\mathbb{F}_q[\alpha] : \mathbb{F}_q] \times [\mathbb{F}_q : \mathbb{F}_p] = [\mathbb{F}_q[\alpha] : \mathbb{F}_q] \times m.$$

Thus $[\mathbb{F}_q[\alpha] : \mathbb{F}_q] = n$. Moreover g is the minimal polynomial of α on \mathbb{F}_q , thus $\deg(g) = n$.

Conclusion: if F is a field with $q = p^m$ elements, there exist irreducible polynomials in $F[x]$ of degree n for all positive integers n . \square

Ex. 7.15 Let $x^n - 1 \in F[x]$, where F is a finite field with q elements. Suppose that $(q, n) = 1$. Show that $x^n - 1$ splits into linear factors in some extension field and that the least degree of such a field is the smallest integer f such that $q^f \equiv 1 \pmod{n}$.

Proof. From exercise 7.12, we know that $x^n - 1$ splits into linear factors in some extension field K , with $[K : F] < \infty$:

$$u(x) = x^n - 1 = (x - \zeta_0)(x - \zeta_1) \cdots (x - \zeta_{n-1}), \quad \zeta_i \in K.$$

Then $u'(x) \wedge u(x) = nx^{n-1} \wedge (x^n - 1) = 1$, since $x(nx^{n-1}) - n(x^n - 1) = n$, and $n \neq 0$ in the field F , because we know from the hypothesis $q \wedge n = 1$ that the characteristic p doesn't divide n . So the n roots of $x^n - 1$ are distinct.

The set $G = \{x \in K \mid x^n = 1\}$ is a subgroup of K^* , thus G is cyclic of order n . Let ζ a generator of G . Then

$$x^n - 1 = (x - 1)(x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{n-1}).$$

Let $p(x)$ be the minimal polynomial of ζ on F , and f the degree of p :

$$f = \deg(p) = [F[\zeta] : F].$$

Thus $\text{Card } F[\zeta] = q^f$, and since $\zeta \in F[\zeta]^*$, $\zeta^{q^f - 1} - 1 = 0$. As the order of ζ in the group G is n , $n \mid q^f - 1$, namely $q^f \equiv 1 \pmod{n}$.

Let k be any positive integer such that $q^k \equiv 1 \pmod{n}$.

Then $n \mid q^k - 1$, thus $\zeta^{q^k - 1} - 1 = 0$, and $\zeta^{q^k} - \zeta = 0$. Let L be any extension of K such that $x^{q^k} - x$ splits in linear factors in L , and let $M = \{\alpha \in L \mid \alpha^{q^k} = \alpha\}$. We know that M is a subfield of L (see Ex. 13), with cardinality q^k , so that $[M : F] = k$. As $\zeta^{q^k} - \zeta = 0$, ζ belongs to M . Therefore $F[\zeta] \subset M$, thus $f = [F[\zeta] : F] \leq k = [M : F]$.

So $f = [F[\zeta] : F]$ is the smallest $k \in \mathbb{N}^*$ such that $q^k \equiv 1 \pmod{n}$.

If K is any extension of F containing the roots of $x^n - 1$, then $K \supset F[\zeta]$, where ζ is a primitive root of unity, so $[K : F] \geq [F[\zeta] : F] = f$.

Conclusion: the minimal degree of an extension $K \supset F$ containing the roots of $x^n - 1$, with $n \wedge q = 1$, is the smallest positive integer f such that $q^f \equiv 1 \pmod{n}$, the order of q modulo n . \square

Ex. 7.16 Calculate the monic irreducible polynomials of degree 4 in $\mathbb{Z}/2\mathbb{Z}[x]$.

Proof. Write F_d the product of irreducible monic polynomials in $\mathbb{F}_2[x]$.

Theorem 2 gives

$$x^{16} - x = x^{2^4} - x = \prod_{d|4} F_d(x) = F_1(x)F_2(x)F_4(x)$$

and

$$x^4 - x = x^{2^2} - x = \prod_{d|2} F_d(x) = F_1(x)F_2(x)$$

$$\text{so } F_4(x) = \frac{x^{16} - x}{x^4 - x} = \frac{x^{15} - 1}{x^3 - 1} = x^{12} + x^9 + x^6 + x^3 + 1,$$

$$F_4(x) = (x^4 + x^3 + x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1).$$

Among the 16 monic polynomials of degree 4 in $\mathbb{F}_2[x]$, 3 are irreducible :

$$P_1(x) = x^4 + x^3 + x^2 + x + 1,$$

$$P_2(x) = x^4 + x + 1,$$

$$P_3(x) = x^4 + x^3 + 1.$$

With sage :

```
sage: A = PolynomialRing(GF(2), 'x')
sage: x = A.gen()
sage: f = (x^16-x)/(x^4-x)
sage: factor(f)
(x^4 + x + 1) * (x^4 + x^3 + 1) * (x^4 + x^3 + x^2 + x + 1)
```

□

Ex. 7.17 Let q and p be distinct odd primes. Show that the number of monic irreducibles of degree q in $\mathbb{Z}/p\mathbb{Z}$ is $q^{-1}(p^q - p)$.

Proof. From Theorem 2 Corollary 2, we know that the number of irreducible polynomials on \mathbb{F}_p of degree q is given by

$$N_q = \frac{1}{q} \sum_{d|q} \mu\left(\frac{q}{d}\right) p^d.$$

As q is prime, d takes the values 1, q , with $\mu(1) = 1, \mu(q) = -1$, so

$$N_q = \frac{p^q - p}{q}.$$

□

Ex. 7.18 Let p be a prime with $p \equiv 3 \pmod{4}$. Show that the residue classes modulo p in $\mathbb{Z}[i]$ form a field with p^2 elements.

Proof. If p is a prime rational integer, with $p \equiv 3 \pmod{4}$, then p is a prime in $\mathbb{Z}[i]$.

Indeed, p is irreducible : if $p = uv$, $u, v \in \mathbb{Z}[i]$, where $u = c + di, v$ are not units, then $p^2 = N(u)N(v)$, $N(u) > 1, N(v) > 1$, so $p = N(u) = u\bar{u} = c^2 + d^2$.

As $c^2 \equiv 0, 1 \pmod{4}, d^2 \equiv 0, 1 \pmod{4}$, so $p \equiv 1 \pmod{4}$, which is in contradiction with the hypothesis.

So p is irreducible in $\mathbb{Z}[i]$, and since $\mathbb{Z}[i]$ is a principal ideal domain, p is prime in $\mathbb{Z}[i]$, thus $\mathbb{Z}[i]/(p)$ is a field.

Let $z = a + bi \in \mathbb{Z}[i]$. The Euclidean division of a, b by p gives

$$a = qp + r, \quad 0 \leq r < p, \quad b = q'p + s, \quad 0 \leq s < p,$$

so

$$z \equiv r + is \pmod{p}, \quad 0 \leq r < p, \quad 0 \leq s < p.$$

Let's verify that these p^2 elements are in different classes of congruences modulo p .

If $r + is \equiv r' + is' \pmod{p}$, then $(r - r')/p + i(s - s')/p \in \mathbb{Z}[i]$, so $r \equiv r', s \equiv s' \pmod{p}$.

As r, r', s, s' are between 0 and $p - 1$, $r = r', s = s'$.

So the cardinality of the field $\mathbb{Z}[i]/(p)$ is p^2 .

□

Ex. 7.19 Let F be a finite field with q elements. If $f(x) \in F[x]$ has degree t , put $|f| = q^t$. Verify the formal identity $\sum_f |f|^{-s} = (1 - q^{1-s})^{-1}$. The sum is over all monic polynomials.

Proof. Let U be the set of monic polynomials in $\mathbb{F}_q[x]$, and U_t the set of monic polynomials of degree t , and $s \in \mathbb{C}$. Then $U = \coprod_{t \in \mathbb{N}} U_t$, so

$$\begin{aligned} \sum_{f \in U} |f|^{-s} &= \sum_{t=0}^{\infty} \sum_{f \in U_t} |f|^{-s} \\ &= \sum_{t=0}^{\infty} \frac{1}{q^{ts}} \sum_{f \in U_t} 1. \end{aligned}$$

As $\sum_{f \in U_t} 1 = \text{Card}(U_t) = q^t$, then, for $\text{Re}(s) > 1$

$$\begin{aligned} \sum_{f \in U} |f|^{-s} &= \sum_{t=0}^{\infty} \frac{1}{q^{t(s-1)}} \\ &= \frac{1}{1 - \frac{1}{q^{s-1}}} \\ &= (1 - q^{1-s})^{-1}. \end{aligned}$$

As $\left| \frac{1}{q^{t(s-1)}} \right| = \frac{1}{q^{t(\text{Re}(s)-1)}}$, the sum is absolutely convergent for $\text{Re}(s) > 1$. This justifies the grouping of terms in this sum.

Conclusion: if $\text{Re}(s) > 1$,

$$\sum_{f \in U} |f|^{-s} = (1 - q^{1-s})^{-1},$$

where U is the set of monic polynomials in $\mathbb{F}_q[x]$. □

Ex. 7.20 With the notation of Exercise 19 let $d(f)$ be the number of monic divisors of f and $\sigma(f) = \sum_{g|f} |g|$, where the sum is over the monic divisors of f . Verify the following identities :

$$(a) \sum_f d(f) |f|^{-s} = (1 - q^{1-s})^{-2}.$$

$$(b) \sum \sigma(f) |f|^{-s} = (1 - q^{1-s})^{-1} (1 - q^{2-s})^{-1}.$$

Proof. (a) With the notation of 7.19, for $s \in \mathbb{C}, \text{Re}(s) > 1$, $\sum_{f \in U} |f|^{-s}$ is absolutely convergent and

$$(1 - q^{1-s})^{-1} = \sum_{f \in U} |f|^{-s}.$$

Then

$$\begin{aligned} (1 - q^{1-s})^{-2} &= \sum_{f \in U} |f|^{-s} \sum_{g \in U} |g|^{-s} \\ &= \sum_{(f,g) \in U^2} |fg|^{-s} \\ &= \sum_{h \in U} \sum_{g \in U, g|h} |h|^{-s}, \end{aligned}$$

indeed, the application

$$\varphi : \begin{cases} U \times U & \rightarrow \{ (h, g) \in U \times U, g \mid h \} \\ (f, g) & \mapsto (fg, g) \end{cases}$$

is a bijection.

So

$$\begin{aligned} (1 - q^{1-s})^{-2} &= \sum_{h \in U} |h|^{-s} \text{Card}\{g \in U, g \mid h\} \\ &= \sum_{h \in U} |h|^{-s} d(h) \\ &= \sum_{f \in U} d(f) |f|^{-s}. \end{aligned}$$

(b) Similarly,

$$\begin{aligned} (1 - q^{1-s})^{-1} (1 - q^{2-s})^{-1} &= \sum_{f \in U} |f|^{-s} \sum_{g \in U} |g|^{-s+1} \\ &= \sum_{(f, g) \in U^2} |g| |fg|^{-s} \\ &= \sum_{h \in U} \sum_{g \in U, g \mid h} |g| |h|^{-s} \\ &= \sum_{h \in U} |h|^{-s} \sum_{g \in U, g \mid h} |g| \\ &= \sum_{h \in U} \sigma(h) |h|^{-s} \\ &= \sum_{f \in U} \sigma(f) |f|^{-s}. \end{aligned}$$

□

Ex. 7.21 Let F be a field with $q = p^n$ elements. For $\alpha \in F$ set $f(x) = (x - \alpha)(x - \alpha^p)(x - \alpha^{p^2}) \cdots (x - \alpha^{p^{n-1}})$. Show that $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$. In particular, $\alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$ and $\alpha\alpha^p\alpha^{p^2} \cdots \alpha^{p^{n-1}}$ are in $\mathbb{Z}/p\mathbb{Z}$.

Proof. Let $F : \begin{cases} \mathbb{F}_q & \rightarrow \mathbb{F}_q \\ x & \mapsto x^p \end{cases}$.

As the characteristic of \mathbb{F}_q is p , $(x + y)^p = x^p + y^p$ et $(xy)^p = x^p y^p$, and each homomorphism of field is injective, so F is a field automorphism (Frobenius automorphism).

For every automorphism H in \mathbb{F}_q , and every polynomial $p(x) = \sum a_i x^i \in \mathbb{F}_q[x]$, write $(H \cdot p)(x) = \sum_i H(a_i) x^i$. Then for all $(p, q) \in \mathbb{F}_q[x]^2$, $H \cdot (pq) = (H \cdot p)(H \cdot q)$.

With this notation,

$$\begin{aligned} f(x) &= (x - \alpha)(x - F\alpha)(x - F^2\alpha) \cdots (x - F^{n-1}\alpha), \\ (F \cdot f)(x) &= (x - F\alpha)(x - F^2\alpha)(x - F^3\alpha) \cdots (x - F^n\alpha). \end{aligned}$$

Since $\alpha \in \mathbb{F}_{p^n}$, $F^n \alpha = \alpha^{p^n} = \alpha$, thus

$$F \cdot f = f.$$

In other words, if $f(x) = \sum_i a_i x^i$, then for all i , $F(a_i) = a_i$, so $a_i^p = a_i$, thus $a_i \in \mathbb{F}_p$, and $f \in \mathbb{F}_p[x]$. In particular, the coefficients $a_{n-1} = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$, $a_0 = \alpha \alpha^p \alpha^{p^2} \cdots \alpha^{p^{n-1}}$ are in \mathbb{F}_p . \square

Ex. 7.22 (continuation) Set $\text{tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$. Prove that

$$(a) \text{tr}(\alpha) + \text{tr}(\beta) = \text{tr}(\alpha + \beta).$$

$$(b) \text{tr}(a\alpha) = a \text{tr}(\alpha) \text{ for } a \in \mathbb{Z}/p\mathbb{Z}.$$

$$(c) \text{ There is an } \alpha \in F \text{ such that } \text{tr}(\alpha) \neq 0.$$

Proof. Let F the Frobenius automorphism of \mathbb{F}_q introduced in Ex.7.21.

(a),(b) : If $x, y \in \mathbb{F}_q$, and $a \in \mathbb{F}_p$, then $a^p = a$, so $F(x + y) = (x + y)^p = x^p + y^p = F(x) + F(y)$, and $F(ax) = a^p x^p = ax^p = aF(x)$, so F is \mathbb{F}_p -linear, and also $\text{tr} = I + F + F^2 + \cdots + F^{n-1}$.

(c) The polynomial $p(x) = x + x^p + x^{p^2} + \cdots + x^{p^{n-1}}$ has degree p^{n-1} , so $p(x)$ has at most p^{n-1} roots in \mathbb{F}_q , and $|\mathbb{F}_q| = p^n > \deg(p) = p^{n-1}$. Therefore there exists in \mathbb{F}_q some element α which is not a root of $p(x)$, and so $\text{tr}(\alpha) = p(\alpha) \neq 0$. \square

Ex. 7.23 (continuation) For $\alpha \in F$ consider the polynomial $x^p - x - \alpha \in F[x]$. Show that this polynomial is either irreducible or the product of linear factors. Prove that the latter alternative holds iff $\text{tr}(\alpha) = 0$.

Proof. Let $f(x) = x^p - x - \alpha \in F[x]$. There exists an extension $K \supset F$ with finite degree on F which contains a root γ of f .

As $\gamma^p - \gamma - \alpha = 0$, then for all $i \in \mathbb{F}_p$,

$$(\gamma + i)^p - (\gamma + i) - \alpha = (\gamma^p - \gamma - \alpha) + i^p - i = 0.$$

So f has n distinct roots in K : $\gamma, \gamma + 1, \dots, \gamma + p - 1$, and so

$$f(x) = (x - \gamma)(x - \gamma - 1) \cdots (x - \gamma - (p - 1)).$$

$F[\gamma]$ contains all roots of f .

- If $\gamma \in F$, $f(x)$ splits in linear factors in F . $f(x)$ is not irreducible, since $\deg(f) = p > 1$.

- If $\gamma \notin F$, we will show that f is irreducible in $F[x]$.

If not, then $f(x) = g(x)h(x)$ is the product of two monic polynomials $g, h \in F[x]$ such that $1 \leq \deg(g) \leq p - 1$.

The unicity of the decomposition in irreducible factors in $F[\gamma][x]$ shows that

$$g(x) = \prod_{i \in A} (x - \gamma - i),$$

where A is a subset of \mathbb{F}_p , with $A \neq \emptyset, A \neq \mathbb{F}_p$. As $g(x) \in F[x]$, $\sum_{i \in A} (\gamma + i) = k\gamma + l \in \mathbb{F}_p$,

where $1 \leq k = |A| \leq p - 1$ and $l = \sum_{i \in A} i \in \mathbb{F}_p$.

So $k\gamma \in \mathbb{F}_p$. Since $\gamma \notin \mathbb{F}_p$, k is not invertible in \mathbb{F}_p , in contradiction with $1 \leq k \leq p-1$. Consequently, $f(x)$ is irreducible.

We conclude that $x^p - x - \alpha \in F[x]$ is irreducible iff $\gamma \notin F$.

Let F be the Frobenius automorphism of K (cf. Ex. 7.21).

$$\alpha = F(\gamma) - \gamma, F(\alpha) = F^2(\gamma) - F(\gamma), \dots, F^{n-1}(\alpha) = F^n(\gamma) - F^{n-1}(\gamma).$$

The sum of these equalities gives

$$\text{tr}(\alpha) = \alpha + F(\alpha) + \dots + F^{n-1}(\alpha) = F^n(\gamma) - \gamma = \gamma^{p^n} - \gamma.$$

As the cardinality of F is $q = p^n$,

$$\gamma \in F \iff \gamma^{p^n} - \gamma = 0 \iff \text{tr}(\alpha) = 0.$$

Conclusion : $x^p - x - \alpha$ is irreducible iff $\text{tr}(\alpha) \neq 0$. If $\text{tr}(\alpha) = 0$, $x^p - x - \alpha$ splits in linear factors in $F[x]$. \square

Ex. 7.24 Suppose that $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ has the property that $f(x+y) = f(x) + f(y) \in \mathbb{Z}/p\mathbb{Z}[x, y]$. Show that $f(x)$ must be of the form $a_0x + a_1x^p + a_2x^{p^2} + \dots + a_mx^{p^m}$.

Lemma If the prime number p divides all binomial coefficients $\binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n-1}$, then n is a power of p .

Proof. Let $u(x) = (x+1)^n - x^n - 1 \in \mathbb{F}_p[x]$. Then $u(x) = \sum_{k=1}^{n-1} \binom{n}{k} x^k = 0$.

Write $n = p^a q$, with $p \wedge q = 1$. We must show that $q = 1$. Suppose at the contrary that $q > 1$. Then

$$u(x) = 0 = (x+1)^{p^a q} - x^{p^a q} - 1 = (x^{p^a} + 1)^q - x^{p^a q} - 1 = \sum_{k=1}^{q-1} \binom{q}{k} x^{kp^a}.$$

Therefore the coefficient $\binom{q}{1} = q$ of x^{p^a} is null in \mathbb{F}_p , thus $p \mid q$: this is absurd. Therefore $q = 1$ and $n = p^a$. \square

Proof. (Ex. 7.24)

Suppose that $f \in \mathbb{F}_p[x]$ verifies the equality $f(x+y) = f(x) + f(y)$ in $\mathbb{F}_p[x, y]$.

Write $f(x) = \sum_{k=1}^d c_k x^k$.

$$\begin{aligned} 0 = f(x+y) - f(x) - f(y) &= \sum_{n=0}^d c_n [(x+y)^n - x^n - y^n] \\ &= \sum_{n=0}^d \sum_{k=1}^{n-1} c_n \binom{n}{k} x^k y^{n-k} \end{aligned}$$

Therefore, for all n , for all k , $1 \leq k \leq n-1$, $c_n \binom{n}{k} = 0$ in \mathbb{F}_p .

From the lemma, if n is not a power of p , there exists a k , $1 \leq k \leq n-1$ such that $\binom{n}{k} \not\equiv 0 \pmod{p}$, thus $c_n = 0$. If we write $a_k = c_{p^k}$, then $f(x)$ is of the form

$$f(x) = a_0x + a_1x^p + a_2x^{p^2} + \dots + a_mx^{p^m}.$$

\square

Chapter 8

Ex. 8.1 Let p be a prime and $d = (m, p-1)$. Prove that $N(x^m = a) = \sum \chi(a)$, the sum being over all χ such that $\chi^d = \varepsilon$.

Proof. Let $d = m \wedge (p-1)$. We prove that $N(x^m = a) = N(x^d = a)$ for all $d \in \mathbb{F}_p$.

- If $a = 0$, 0 is the only root of $x^m - a$ or $x^d - a$, so $N(x^m = a) = N(x^d = a) = 1$.
- If $a \in \mathbb{F}_p^*$ and $x^m = a$ has a solution, then we know from the demonstration of Proposition 4.2.1 that $N(x^m = a) = d$, and $N(x^d = a) = d \wedge (p-1) = d$, thus $N(x^m = a) = N(x^d = a)$.
- If $a \in \mathbb{F}_p^*$ and $x^m = a$ has no solution, then (Prop. 4.2.1) $a^{(p-1)/d} \neq 1$, thus $x^d = a$ has no solution : $N(x^m = a) = 0 = N(x^d = a)$.

Using Prop. 8.1.5, as $d \mid p-1$, we obtain

$$N(x^m = a) = N(x^d = a) = \sum_{\chi^d = \varepsilon} \chi(a).$$

□

Ex. 8.2, false sentence. With the notation of Exercise 1 show that $N(x^m = a) = N(x^d = a)$ and conclude that if $d_i = (m_i, p-1)$, then $\sum_i a_i x^{m_i} = b$ and $\sum_i a_i x^{d_i} = b$ have the same number of solutions.

This result is false. I give a counterexample with $p = 5$: $x + x^3 = 0 \in \mathbb{F}_5[x]$ has 3 solutions 0, 2, -2. As $3 \wedge (p-1) = 3 \wedge 4 = 1$, the reduced equation is $x + x = 0$, which has an unique solution 0. The true sentence is :

Ex. 8.2 With the notation of Exercise 1 show that $N(x^m = a) = N(x^d = a)$ and conclude that if $d_i = (m_i, p-1)$, then $\sum_i a_i x_i^{m_i} = b$ and $\sum_i a_i x_i^{d_i} = b$ have the same number of solutions.

Proof. From Ex. 8.1, we know that

$$N(x^m = a) = \sum_{\chi^d = \varepsilon} \chi(a) = N(x^d = a).$$

Using this result, we obtain

$$\begin{aligned} N\left(\sum_{i=1}^l a_i x_i^{m_i} = b\right) &= \sum_{a_1 u_1 + \dots + a_l u_l = b} \prod_{i=1}^l N(x^{m_i} = u_i) \\ &= \sum_{a_1 u_1 + \dots + a_l u_l = b} \prod_{i=1}^l N(x^{d_i} = u_i) \\ &= N\left(\sum_{i=1}^l a_i x_i^{d_i} = b\right). \end{aligned}$$

□

Ex. 8.3 Let χ be a non trivial multiplicative character of \mathbb{F}_p and ρ be the character of order 2. Show that $\sum_t \chi(1 - t^2) = J(\chi, \rho)$. [Hint: Evaluate $J(\chi, \rho)$ using the relation $N(x^2 = a) = 1 + \rho(a)$.]

Proof.

$$\begin{aligned} J(\chi, \rho) &= \sum_{a+b=1} \chi(a)\rho(b) \\ &= \sum_{a+b=1} \chi(a)(N(x^2 = b) - 1) \\ &= \sum_{a+b=1} \chi(a)N(x^2 = b) - \sum_{a+b=1} \chi(a). \end{aligned}$$

As $\chi \neq \varepsilon$,

$$\sum_{a+b=1} \chi(a) = \sum_{a \in \mathbb{F}_p} \chi(a) = 0.$$

Let $C = \{x^2 \mid x \in \mathbb{F}_p^*\}$ the set of squares in \mathbb{F}_p^* , \overline{C} its complementary in \mathbb{F}_p^* :

$$\mathbb{F}_p = \{0\} \cup C \cup \overline{C}.$$

Then

$$\begin{aligned} J(\chi, \rho) &= \sum_{a+b=1} \chi(a)N(x^2 = b) \\ &= \sum_{a+b=1, b=0} \chi(a)N(x^2 = b) + \sum_{a+b=1, b \in C} \chi(a)N(x^2 = b) + \sum_{a+b=1, b \in \overline{C}} \chi(a)N(x^2 = b) \\ &= \chi(1) + 2 \sum_{b \in C} \chi(1 - b), \end{aligned}$$

because $N(x^2 = b) = 0$ if $x \in \overline{C}$, and $N(x^2 = b) = 2$ if $x \in C$. As each $b \in C$ has two roots, and as the set of roots of two distinct b are disjointed,

$$J(\chi, \rho) = \chi(1) + \sum_{t \in \mathbb{F}_p^*} \chi(1 - t^2) = \sum_{t \in \mathbb{F}_p} \chi(1 - t^2).$$

Conclusion : if χ is a non trivial multiplicative character of \mathbb{F}_p and ρ the character of order 2,

$$J(\chi, \rho) = \sum_{t \in \mathbb{F}_p} \chi(1 - t^2).$$

□

Ex. 8.4 Show, if $k \in \mathbb{F}_p, k \neq 0$, that $\sum_t \chi(t(k - t)) = \chi(k^2/2^2)J(\chi, \rho)$.

Proof. We know from Ex. 8.3 that $J(\chi, \rho) = \sum_t \chi(1 - t^2)$, so

$$\begin{aligned}
J(\chi, \rho) &= \sum_{t \in \mathbb{F}_p} \chi(1-t)\chi(1+t) \\
&= \sum_{u \in \mathbb{F}_p} \chi(u)\chi(2-u) \quad (u = 1-t) \\
&= \chi(2^2) \sum_{u \in \mathbb{F}_p} \chi\left(\frac{u}{2}\right) \chi\left(1 - \frac{u}{2}\right) \\
&= \chi(2^2) \sum_{v \in \mathbb{F}_p} \chi(v)\chi(1-v) \quad (u = 2v) \\
&= \chi(2^2)\chi(k^{-2}) \sum_{w \in \mathbb{F}_p} \chi(kw)\chi(k-kw) \\
&= \chi(2^2/k^2) \sum_{t \in \mathbb{F}_p} \chi(t)\chi(k-t) \quad (t = kw).
\end{aligned}$$

Conclusion: if $k \in \mathbb{F}^*$, and χ is a non trivial character, ρ the character of order 2,

$$\sum_{t \in \mathbb{F}_p} \chi(t(k-t)) = \chi(k^2/2^2)J(\chi, \rho).$$

□

Ex. 8.5 If $\chi^2 \neq \varepsilon$, show that $g(\chi)^2 = \chi(2)^{-2}J(\chi, \rho)g(\chi^2)$. [Hint: Write out $g(\chi)^2$ explicitly and use Exercise 4.]

Proof. Let $\zeta = e^{2i\pi/p}$. Using the result of Ex. 8.4, we obtain

$$\begin{aligned}
g(\chi)^2 &= \left(\sum_t \chi(t)\zeta^t \right) \left(\sum_s \chi(s)\zeta^s \right) \\
&= \sum_{s,t} \chi(t)\chi(s)\zeta^{t+s} \\
&= \sum_k \left(\sum_{s+t=k} \chi(t)\chi(s) \right) \zeta^k \\
&= \sum_k \left(\sum_t \chi(t(k-t)) \right) \zeta^k \\
&= \chi(-1) \sum_t \chi(t^2) + \sum_{k \neq 0} \chi(k^2/2^2)J(\chi, \rho)\zeta^k \\
&= \chi(-1) \sum_t \chi^2(t) + \chi(2)^{-2}J(\chi, \rho) \sum_{k \neq 0} \chi^2(k)\zeta^k
\end{aligned}$$

If $\chi^2 \neq \varepsilon$, $\sum_t \chi^2(t) = 0$, so

$$g(\chi)^2 = \chi(2)^{-2}J(\chi, \rho)g(\chi^2).$$

□

Ex. 8.6 (continuation) Show that $J(\chi, \chi) = \chi(2)^{-2} J(\chi, \rho)$.

Proof. As $\chi^2 \neq \varepsilon$, Theorem 1 Chapter 8 gives $J(\chi, \chi) = g(\chi)^2/g(\chi^2)$, and Exercise 8.5 gives $g(\chi)^2/g(\chi^2) = \chi(2)^{-2} J(\chi, \rho)$, so

$$J(\chi, \chi) = \chi(2)^{-2} J(\chi, \rho).$$

□

Ex. 8.7 Suppose that $p \equiv 1 \pmod{4}$ and that χ is a character of order 4. Then $\chi^2 = \rho$ and $J(\chi, \chi) = \chi(-1)J(\chi, \rho)$. [Hint: Evaluate $g(\chi)^4$ in two ways.]

Proof. As χ is a character of order 4, χ^2 is a character of order 2, and ρ (Legendre's character) is the unique character of order 2, so $\chi^2 = \rho$.

From Prop. 8.3.3 we have

$$g(\chi)^4 = \chi(-1)pJ(\chi, \chi)J(\chi, \chi^2) = \chi(-1)pJ(\chi, \chi)J(\chi, \rho).$$

Squaring the result of Ex. 8.5, we obtain

$$g(\chi)^4 = \chi(2)^{-4} J(\chi, \rho)^2 [g(\chi^2)]^2.$$

Moreover $\chi(2^4) = \chi^4(2) = \varepsilon(2) = 1$, and $g(\chi^2) = g(\rho) = g$, so $[g(\chi^2)]^2 = g^2 = (-1)^{(p-1)/2} p = p$ (From Prop. 6.3.2 and $p \equiv 1 \pmod{4}$).

Equating these two results, we obtain

$$\chi(-1)pJ(\chi, \chi)J(\chi, \rho) = J(\chi, \rho)^2 p.$$

As $g(\chi)^4 \neq 0$ since $|g(\chi)|^2 = p$, we have $J(\chi, \rho) \neq 0$, so

$$\chi(-1)J(\chi, \chi) = J(\chi, \rho).$$

$[\chi(-1)]^2 = \chi((-1)^2) = \chi(1) = 1$, so $\chi(-1) = \pm 1$, and $\chi(-1)^{-1} = \chi(-1)$, thus

$$J(\chi, \chi) = \chi(-1)J(\chi, \rho).$$

□

Ex. 8.8 Generalize Exercise 3 in the following way. Suppose that p is a prime, $\sum_t \chi(1 - t^m) = \sum_\lambda J(\chi, \lambda)$, where λ varies over all characters such that $\lambda^m = \varepsilon$. Conclude that $|\sum_t \chi(1 - t^m)| \leq (m-1)p^{1/2}$.

Proof. For all $y \in \mathbb{F}_p$, write $A_y = \{x \in \mathbb{F}_p \mid x^m = y\}$. Then $|A_y| = N(x^m = y)$.

$\mathbb{F}_p = \coprod_{y \in \mathbb{F}_p} A_y$ is the disjoint union of the A_y :

- if $x \in A_y \cap A_{y'}$, then $x^m = y = y'$. This proves

$$y \neq y' \Rightarrow A_y \cap A_{y'} = \emptyset.$$

- Every $x \in \mathbb{F}_p$ satisfies $x \in A_{x^m}$, thus

$$\bigcup_{y \in \mathbb{F}_p} A_y = \mathbb{F}_p.$$

(Note that some A_y may be empty.)

Therefore

$$\sum_{t \in \mathbb{F}_p} \chi(1 - t^m) = \sum_{y \in \mathbb{F}_p} \sum_{t \in A_y} \chi(1 - t^m) = \sum_{y \in \mathbb{F}_p} |A_y| \chi(1 - y) = \sum_{y \in \mathbb{F}_p} N(x^m = y) \chi(1 - y).$$

Moreover, $N(x^m = y) = \sum_{\lambda^m = \varepsilon} \lambda(y)$ (Prop. 8.1.5), so

$$\begin{aligned} \sum_{t \in \mathbb{F}_p} \chi(1 - t^m) &= \sum_{y \in \mathbb{F}_p} \sum_{\lambda^m = \varepsilon} \lambda(y) \chi(1 - y) \\ &= \sum_{\lambda^m = \varepsilon} \sum_{x+y=1} \chi(x) \lambda(y) \\ &= \sum_{\lambda^m = \varepsilon} J(\chi, \lambda). \end{aligned}$$

Conclusion :

$$\sum_{t \in \mathbb{F}_p} \chi(1 - t^m) = \sum_{\lambda^m = \varepsilon} J(\chi, \lambda).$$

We know that there exist m characters whose order divides m . We know that $\chi \neq \varepsilon$, $J(\chi, \varepsilon) = 0$, and $|J(\chi, \lambda)| = \sqrt{p}$ for every $\lambda \neq \varepsilon, \lambda \neq \chi^{-1}$ (Theorem 1 and Corollary).

Moreover, by Theorem 1(c), $|J(\chi, \chi^{-1})| = 1 \leq \sqrt{p}$, so

$$\left| \sum_{t \in \mathbb{F}_p} \chi(1 - t^m) \right| \leq \sum_{\lambda^m = \varepsilon, \lambda \neq \varepsilon} |J(\chi, \lambda)| \leq (m-1)\sqrt{p}.$$

□

Ex. 8.9 Suppose that $p \equiv 1 \pmod{3}$ and that χ is a character of order 3. Prove (using Exercise 5) that $g(\chi)^3 = p\pi$, where $\pi = \chi(2)J(\chi, \rho)$.

Proof. As χ is a character of order 3, $\chi^2 \neq \varepsilon$. From Exercise 5, we know that

$$g(\chi)^2 = \chi(2)^{-2} J(\chi, \rho) g(\chi^2).$$

So

$$g(\chi)^3 = \chi(2)^{-2} J(\chi, \rho) g(\chi^2) g(\chi).$$

Recall (§8.2) that

$$\overline{g(\chi)} = \sum_t \overline{\chi(t)} \zeta^{-t} = \chi(-1) \sum_t \overline{\chi(-t)} \zeta(-t) = \chi(-1) g(\bar{\chi}),$$

Here $\chi(-1) = 1$, because $\chi(-1) = \chi((-1)^3) = \chi^3(-1) = \varepsilon(-1) = 1$. Hence

$$g(\chi^2) g(\chi) = g(\bar{\chi}) g(\chi) = \overline{g(\chi)} g(\chi) = |g(\chi)|^2 = p.$$

Moreover $\chi(2)^3 = \chi^3(2) = 1$, so $\chi(2)^{-2} = \chi(2)$.

Conclusion : if χ is a character of order 3,

$$g(\chi)^3 = p\pi, \text{ where } \pi = \chi(2)J(\chi, \rho).$$

□

Ex. 8.10 (continuation) Show that $\chi\rho$ is a character of order 6 and that

$$g(\chi\rho)^6 = (-1)^{(p-1)/2} p\bar{\pi}^4.$$

Proof. $(\chi\rho)^6 = \chi^6\rho^6 = \varepsilon$, $(\chi\rho)^2 = \chi^2 \neq \varepsilon$, $(\chi\rho)^3 = \rho^3 = \rho \neq \varepsilon$, so $\chi\rho$ is of order 6.

$J(\chi, \rho)g(\chi\rho) = g(\chi)g(\rho)$ since $\chi, \rho, \chi\rho$ are non trivial characters. So

$$g(\chi\rho)^6 = \frac{g(\chi)^6 g(\rho)^6}{J(\chi, \rho)^6}.$$

From Exercise 8.9, $g(\chi)^6 = p^2\pi^2$. Proposition 6.3.2 gives $g(\rho)^2 = (-1)^{(p-1)/2}p$, so $g(\rho)^6 = (-1)^{(p-1)/2}p^3$. As $\pi = \chi(2)J(\chi, \rho)$, $J(\chi, \rho)^6 = \chi(2)^{-6}\pi^6 = \pi^6$, since $\chi(2)^3 = 1$. Therefore

$$g(\chi\rho)^6 = \frac{p^2\pi^2(-1)^{(p-1)/2}p^3}{\pi^6} = (-1)^{(p-1)/2}p^5\pi^{-4}.$$

Moreover, $\pi\bar{\pi} = \chi(2)\overline{\chi(2)}J(\chi, \rho)\overline{J(\chi, \rho)} = |J(\chi, \rho)|^2 = p$ (Theorem 8.1, Corollary), so $\pi^{-1} = \bar{\pi}/p$. In conclusion,

$$g(\chi\rho)^6 = (-1)^{(p-1)/2} p\bar{\pi}^4.$$

□

Ex. 8.11 Use Gauss' theorem to find the number of solutions to $x^3 + y^3 = 1$ in \mathbb{F}_p for $p = 13, 19, 37$, and 97.

Proof. • $p = 13$.

$4 \times 13 = 52 = (-5)^2 + 27 \times 1^2$, where $-5 \equiv 1 \pmod{3}$, so $A = -5$.

If $p = 13$, $N(x^3 + y^3 = 1) = p - 2 + A = 13 - 2 - 5 = 6$: the solutions are only the trivial solutions.

• $p = 19$.

$4 \times 19 = 76 = 7^2 + 27 \times 1^2$, where $7 \equiv 1 \pmod{3}$, so $A = 7$.

If $p = 19$, $N(x^3 + y^3 = 1) = 19 - 2 + 7 = 24$.

• $p = 37$.

$4 \times 37 = 148 = (-11)^2 + 27 \times 1^2$, where $-11 \equiv 1 \pmod{3}$, so $A = -11$.

If $p = 37$, $N(x^3 + y^3 = 1) = 37 - 2 - 11 = 24$.

• $p = 97$.

$4 \times 97 = 388 = 19^2 + 27 \times 1^2$, where $19 \equiv 1 \pmod{3}$, so $A = 19$.

If $p = 97$, $N(x^3 + y^3 = 1) = 97 - 2 + 19 = 114$.

(These results were verified on pari/gp.)

□

Ex. 8.12 If $p \equiv 1 \pmod{4}$, then we have seen that $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$. If we require that a and b are positive, that a be odd, and that b is even, show that a and b are uniquely determined. (Hint: Use the fact that unique factorization holds in $\mathbb{Z}[i]$ and that if $p = a^2 + b^2$ then $a + bi$ is a prime in $\mathbb{Z}[i]$.)

Proof. Suppose that p is prime, $p \equiv 1 \pmod{4}$, and $p = a^2 + b^2 = c^2 + d^2$, where a, b, c, d are positive integers, a, c odd, b, d even. We will show that $a = c, b = d$.

As $p = N(a + bi)$, $\pi = a + bi$ is irreducible in $\mathbb{Z}[i]$: indeed $\pi = uv$ implies that $p = N(\pi) = N(u)N(v)$, so $N(u) = 1$ or $N(v) = 1$, and u or v is an unit.

Since $\mathbb{Z}[i]$ is a principal ideal domain, π is a prime in $\mathbb{Z}[i]$.

$(a + bi)(a - bi) = (c + di)(c - di)$, so the prime π divides $c + di$, or it divides $c - di$.

As $N(\pi) = N(c + di) = N(c - di)$, the quotient is an unit. Therefore π is an associate of $c + di$ or $c - di$. Since the units in $\mathbb{Z}[i]$ are $1, -1, i, -i$,

$$a + bi = \pm(c + di), \text{ or } a + bi = \pm i(c + di), \text{ or } a + bi = \pm(c - di), \text{ or } a + bi = \pm i(c - di).$$

In all cases, $a = \pm c, b = \pm d$, or $a = \pm d, b = \pm c$. Since a, b, c, d are positive, $a = c, b = d$, or $a = d, b = c$. As a, c are odds, and b, d even, $a = c, b = d$: the unicity of the decomposition is proved. \square

Ex. 8.13 If $p \equiv 1 \pmod{3}$, we have seen that $4p = A^2 + 27B^2$, with $A, B \in \mathbb{Z}$. If we require that $A \equiv 1 \pmod{3}$, show that A is uniquely determined. (Hint: Use the fact that unique factorization holds in $\mathbb{Z}[\omega]$. This proof is a little trickier than that for Exercise 12.)

Proof. Suppose that $4p = A^2 + 27B^2 = C^2 + 27D^2$, where $A \equiv C \equiv 1 \pmod{3}$. We will show that $A = C$.

Let $\omega = e^{2i\pi/3} = -1/2 + i\sqrt{3}/2$. Then $i\sqrt{3} = 2\omega + 1$, and for all x, y , $x^3 + 3y^2 = (x + i\sqrt{3}y)(x - i\sqrt{3}y) = (x + (2\omega + 1)y)(x - (2\omega + 1)y)$,

$$x^2 + 3y^2 = (x + y + 2\omega y)(x - y - 2\omega y).$$

With $x = A, y = 3B$, we obtain

$$4p = A^2 + 27B^2 = (A + 3B + 6\omega B)(A - 3B - 6\omega B).$$

Note that A, B are of same parity, since $4p = A^2 + 27B^2$.

So we can write $p = ((A + 3B)/2 + 3\omega B)((A - 3B)/2 - 3\omega B)$:

$$p = \pi\bar{\pi}, \text{ where } \pi = \frac{A + 3B}{2} + 3\omega B \in \mathbb{Z}[\omega].$$

π is a prime in $\mathbb{Z}[\omega]$: indeed $\pi = uv$, $u, v \in \mathbb{Z}[\omega]$ implies $p = N(\pi) = N(u)N(v)$, then $N(u) = 1$ or $N(v) = 1$, u or v is an unit, so π is irreducible in the principal ideal domain $\mathbb{Z}[\omega]$, thus π is a prime in $\mathbb{Z}[\omega]$.

$$\pi\bar{\pi} = \left(\frac{A + 3B}{2} + 3\omega B\right) \left(\frac{A - 3B}{2} - 3\omega B\right) = \left(\frac{C + 3D}{2} + 3\omega D\right) \left(\frac{C - 3D}{2} - 3\omega D\right).$$

As π is a prime, it divides $\frac{C + 3D}{2} + 3\omega D$ or its conjugate. Since they have the same norm

p , they are associated. The units of $\mathbb{Z}[\omega]$ are $\pm 1, \pm \omega, \pm \omega^2$, so there exists 12 cases :

$$\begin{aligned}\frac{A+3B}{2} + 3\omega B &= \pm \left(\frac{C+3D}{2} + 3\omega D \right), \\ \frac{A+3B}{2} + 3\omega B &= \pm \omega \left(\frac{C+3D}{2} + 3\omega D \right), \\ \frac{A+3B}{2} + 3\omega B &= \pm \omega^2 \left(\frac{C+3D}{2} + 3\omega D \right), \\ \frac{A+3B}{2} + 3\omega B &= \pm \left(\frac{C-3D}{2} - 3\omega D \right), \\ \frac{A+3B}{2} + 3\omega B &= \pm \omega \left(\frac{C-3D}{2} - 3\omega D \right), \\ \frac{A+3B}{2} + 3\omega B &= \pm \omega^2 \left(\frac{C-3D}{2} - 3\omega D \right).\end{aligned}$$

If we replace D by $-D$, we obtain the 6 last cases from the 6 first cases, so it is sufficient to examine the first 6 cases. Recall that $(1, \omega)$ is a \mathbb{Z} -base of $\mathbb{Z}[\omega]$.

1) $A + 3B + 6\omega B = C + 3D + 6\omega D$.

Then $B = D$ and $A + 3B = C + 3D$, so $A = C$, which is the expected result. The five other cases are impossible :

2) $A + 3B + 6\omega B = -C - 3D - 6\omega D$.

Then $B = -D, A = -C$. As $A \equiv C \equiv 1 \pmod{3}$, this is impossible.

3) $A + 3B + 6\omega B = \omega(C + 3D + 6\omega D) = \omega(C + 3D) + (-1 - \omega)6D = -6D + \omega(C - 3D)$.

Then $A + 3B = -6D, A \equiv 0 \pmod{3}$, this is impossible.

4) $A + 3B + 6\omega B = -\omega(C + 3D + 6\omega D) = -\omega(C + 3D) + (1 + \omega)6D = 6D + \omega(-C + 3D)$.

Then $A + 3B = -6D, A \equiv 0 \pmod{3}$, this is impossible.

5) $A + 3B + 6\omega B = \omega^2(C + D + 6\omega D) = (-1 - \omega)(C + 3D) + 6D = -C + 3D + \omega(-C - 3D)$. Then $A + 3B = -C + 3D, A \equiv -C \pmod{3}$, this is impossible.

6) $A + 3B + 6\omega B = -\omega^2(C + 3D + 6\omega D) = (1 + \omega)(C + 3D) - 6D = (C - 3D) + \omega(C + 3D)$.

Then $6B = C + 3D, C \equiv 0 \pmod{3}$, this is impossible.

In conclusion $A = C$. □

Ex. 8.14 Suppose that $p \equiv 1 \pmod{n}$ and that χ is a character of order n . Show that $g(\chi)^n \in \mathbb{Z}[\zeta]$, where $\zeta = e^{2\pi i/n}$.

Proof. From Proposition 8.3.3 we know that

$$g(\chi)^n = \chi(-1)pJ(\chi, \chi)J(\chi, \chi^2) \cdots J(\chi, \chi^{n-2}).$$

Let $\mathbb{U}_n = \{x \in \mathbb{C} \mid x^n = 1\} = \{1, \zeta, \dots, \zeta^{n-1}\}$, with $\zeta = e^{2\pi i/n}$, the group of n -th roots of unity. As the order of χ is n , for all $x \in \mathbb{F}_p^*$, $(\chi(x))^n = \chi^n(x) = \varepsilon(x) = 1$, so $\chi(x) \in \mathbb{U}_n$, and also $\chi^k(x) = (\chi(x))^k$.

Therefore $J(\chi, \chi^k) = \sum_{x+y=1} \chi(x)\chi^k(y) \in \mathbb{Z}[\zeta]$. Moreover $\chi(-1) = \pm 1$, so $\chi(-1)$ and p are in $\mathbb{Z}[\zeta]$. In conclusion $g(\chi)^n \in \mathbb{Z}[\zeta]$. □

Ex. 8.15 Suppose that $p \equiv 1 \pmod{6}$ and let χ and ρ be characters of order 3 and 2, respectively. Show that the number of solutions to $y^2 = x^3 + D$ in \mathbb{F}_p is $p + \pi + \bar{\pi}$, where $\pi = \chi\rho(D)J(\chi\rho)$. If $\chi(2) = 1$, show that the number of solutions to $y^2 = x^3 + 1$ is $p + A$, where $4p = A^2 + 27B^2$ and $A \equiv 1 \pmod{3}$. Verify this result numerically when $p = 31$.

Proof. $x \mapsto -x$ is a bijection between the set of roots of $x^3 = b$ and the set of roots of $(-x)^3 = b$, so $N(x^3 = b) = N((-x)^3 = b) = N(x^3 = -b)$.

As χ is a character of order 3, the characters whose order divides 3 are $\varepsilon, \chi, \chi^2$. Using Prop. 8.1.5, we obtain, if $D \neq 0$,

$$\begin{aligned} N(y^2 = x^3 + D) &= \sum_{a+b=D} N(y^2 = a)N((-x)^3 = b) \\ &= \sum_{a+b=D} N(y^2 = a)N(x^3 = b) \\ &= \sum_{a+b=D} (1 + \rho(a))(1 + \chi(b) + \chi^2(b)) \\ &= \sum_{i=0}^1 \sum_{j=0}^2 \sum_{a+b=D} \rho^i(a)\chi^j(b) \\ &= \sum_{i=0}^1 \sum_{j=0}^2 \rho(D)^i \chi(D)^j \sum_{a'+b'=1} \rho^i(a')\chi^j(b') \quad (a = Da', b = Db') \\ &= \sum_{i=0}^1 \sum_{j=0}^2 \rho(D)^i \chi(D)^j J(\chi^j, \rho^i). \end{aligned}$$

We know (Theorem 1) that $J(\chi, \varepsilon) = J(\chi^2, \varepsilon) = J(\varepsilon, \rho) = 0$, $J(\varepsilon, \varepsilon) = p$, so

$$N(y^2 = x^3 + D) = p + \rho(D)\chi(D)J(\chi, \rho) + \rho(D)\chi^2(D)J(\chi^2, \rho).$$

As $\chi^2(D) = \chi^{-1}(D) = \overline{\chi(D)}$, and as $\overline{\rho(D)} = \rho(D)$, then $J(\chi^2, \rho) = J(\overline{\chi}, \overline{\rho}) = \overline{J(\chi, \rho)}$, and

$$N(y^2 = x^3 + D) = p + \pi + \bar{\pi}, \text{ where } \pi = (\rho\chi)(D)J(\chi, \rho).$$

If $\chi(2) = 1$, then from Exercise 8.6 we have

$$J(\chi, \chi) = \chi(2)^{-2}J(\chi, \rho) = J(\chi, \rho).$$

With $D = 1$ (if $\chi(2) = 1$), we obtain

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

From Prop. 8.3.4 we know that $J(\chi, \chi) = a + b\omega$, $b \equiv 0 \pmod{3}$, $a \equiv -1 \pmod{3}$.

$\pi + \bar{\pi} = 2 \operatorname{Re} J(\chi, \chi) = 2a - b \equiv 1 \pmod{3}$, and $p = |J(\chi, \rho)|^2 = a^2 - ab + b^2$, so $4p = (2a - b)^2 + 3b^2$.

Writing $A = 2a - b$, $B = b/3$, we obtain $4p = A^2 + 27B^2$, $A \equiv 1 \pmod{3}$ (the unicity of A if proved in Exercise 8.13).

Conclusion : $N(y^2 = x^3 + 1) = p + A$, where $4p = A^2 + 27B^2$, $A \equiv 1 \pmod{3}$.

If $p = 31$, 3 is a primitive element, and $2 = 3^{24} = (3^8)^3$ in \mathbb{F}_{31} , therefore $\chi(2) = 1$.

$31 = 4 + 27$, $4 \times 31 = 124 = 4^2 + 27 \times 2^2$, and $4 \equiv 1 \pmod{3}$, so

if $p = 31$, $N(y^2 = x^3 + 1) = 35$. □

Ex. 8.16 Suppose that $p \equiv 1 \pmod{4}$ and that χ is a character of order 4. Let N be the number of solutions to $x^4 + y^4 = 1$ in \mathbb{F}_p . Show that $N = p + 1 - \delta_4(-1)4 + 2 \operatorname{Re} J(\chi, \chi) + 4 \operatorname{Re} J(\chi, \rho)$.

Proof. Let χ be a character of order 4 : such a character exists since $p \equiv 1 \pmod{4}$. Then

$$\begin{aligned}
N(x^4 + y^4 = 1) &= \sum_{a+b=1} N(x^4 = a)N(y^4 = b) \\
&= \sum_{a+b=1} \sum_{i=0}^3 \chi^i(a) \sum_{j=0}^3 \chi^j(b) \\
&= \sum_{i=0}^3 \sum_{j=0}^3 \sum_{a+b=1} \chi^i(a) \chi^j(b) \\
&= \sum_{i=0}^3 \sum_{j=0}^3 J(\chi^i, \chi^j) \\
&= p - \chi(-1) - \chi^2(-1) - \chi^3(-1) \\
&\quad + J(\chi, \chi) + J(\chi, \chi^2) + J(\chi^2, \chi) \\
&\quad + J(\chi^2, \chi^3) + J(\chi^3, \chi^2) + J(\chi^3, \chi^3),
\end{aligned}$$

since from Theorem 1, we have $J(\varepsilon, \varepsilon) = p$, $J(\varepsilon, \chi^j) = 0$ for $j = 1, 2, 3$, and $J(\chi^i, \chi^{4-i}) = -\chi^i(-1)$.

Moreover

$$-[\chi(-1) + \chi^2(-1) + \chi^3(-1)] = 1 - [1 + \chi(-1) + \chi^2(-1) + \chi^3(-1)],$$

and

$$\begin{cases} 1 + \chi(-1) + \chi^2(-1) + \chi^3(-1) = \frac{1-\chi^4(-1)}{1-\chi(-1)} & = 0 \quad \text{if } \chi(-1) \neq 1 \\ & = 4 \quad \text{if } \chi(-1) = 1. \end{cases}$$

Let g a generator of \mathbb{F}_p^* . Recall that $\chi(g) = e^{qi\pi/2}$ with q odd, so $\chi : a = g^k \mapsto e^{iqk\pi/2} = i^{qk}$, thus

$$\chi(a) = 1 \iff \chi(g^k) = 1 \iff i^{qk} = 1 \iff 4 \mid k \iff a = b^4, b \in \mathbb{F}^*.$$

δ_4 is defined by $\delta_4(a) = 1$ if a is a fourth power, 0 if not. Then

$$-[\chi(-1) + \chi^2(-1) + \chi^3(-1)] = 1 - \delta_4(-1)4.$$

Moreover $J(\chi, \chi) + J(\chi^3, \chi^3) = 2 \operatorname{Re} (J(\chi, \chi))$, and

$$J(\chi, \chi^2) + J(\chi^3, \chi^2) + J(\chi^2, \chi) + J(\chi^2, \chi^3) = 2 \operatorname{Re} (J(\chi, \chi^2)) + 2 \operatorname{Re} (J(\chi^2, \chi)) = 4 \operatorname{Re} (J(\chi, \chi^2)).$$

χ is of order 4, so $\rho = \chi^2$ is the unique character of order 2, the Legendre's character.

In conclusion,

$$N(x^4 + y^4 = 1) = p + 1 - \delta_4(-1)4 + 2 \operatorname{Re} (J(\chi, \chi)) + 4 \operatorname{Re} (J(\chi, \rho)).$$

□

Ex. 8.17 (continuation) By Exercise 8.7, $J(\chi, \chi) = \chi(-1)J(\chi, \rho)$. Let $\pi = -J(\chi, \rho)$. Show that

(a) $N = p - 3 - 6 \operatorname{Re} \pi$ if $p \equiv 1 \pmod{8}$.

(b) $N = p + 1 - 2 \operatorname{Re} \pi$ if $p \equiv 5 \pmod{8}$.

Proof. Let g a generator in \mathbb{F}_p^* . As $(g^{(p-1)/2})^2 = 1$ and $g^{(p-1)/2} \neq 1$, then $g^{(p-1)/2} = -1$. As in Exercise 8.16, write $\chi(g) = e^{qi\pi/2}$, with q odd.

Then -1 is a fourth power in \mathbb{F}_p^* iff (see Exercise 8.16)

$$\begin{aligned} \delta_4(-1) = 1 &\iff \chi(-1) = 1 \\ &\iff \chi(g^{(p-1)/2}) = 1 \\ &\iff e^{q((p-1)/2)i\pi/2} = 1 \\ &\iff 4 \mid q(p-1)/2 \\ &\iff 4 \mid (p-1)/2 \\ &\iff p \equiv 1 \pmod{8}. \end{aligned}$$

By Exercise 8.7, as χ is a character of order 4,

$$J(\chi, \chi) = \chi(-1)J(\chi, \rho).$$

- If $p \equiv 1[8]$,
 $\chi(-1) = 1$, so $J(\chi, \chi) = J(\chi, \rho)$, and $\delta_4(-1) = 1$.

$$\begin{aligned} N &= p + 1 - \delta_4(-1)4 + 2 \operatorname{Re} J(\chi, \chi) + 4 \operatorname{Re} J(\chi, \rho) \\ &= p - 3 + 6 \operatorname{Re} J(\chi, \rho) \\ &= p - 3 - 6 \operatorname{Re} \pi, \quad \text{where } \pi = -J(\chi, \rho). \end{aligned}$$

- If $p \equiv 5[8]$,
 $\chi(-1) = -1$, donc $J(\chi, \chi) = -J(\chi, \rho)$, et $\delta_4(-1) = 0$

$$\begin{aligned} N &= p + 1 - \delta_4(-1)4 + 2 \operatorname{Re} J(\chi, \chi) + 4 \operatorname{Re} J(\chi, \rho) \\ &= p + 1 + 2 \operatorname{Re} J(\chi, \rho) \\ &= p + 1 - 2 \operatorname{Re} \pi. \end{aligned}$$

□

Ex. 8.18 (continuation) Let $\pi = a + bi$. One can show (see Chapter 11, Section 5) that a is odd, b is even, and $a \equiv 1 \pmod{4}$ if $4 \mid b$ and $a \equiv -1 \pmod{4}$ if $4 \nmid b$. Let $p = A^2 + B^2$ and fix A by requiring that $A \equiv 1 \pmod{4}$. Then show that

(a) $N = p - 3 - 6A$ if $p \equiv 1 \pmod{8}$,

(b) $N = p + 1 + 2A$ if $p \equiv 5 \pmod{8}$.

Proof. Recall that $\pi = -J(\chi, \rho) \in \mathbb{Z}[i]$, so $\pi = a + bi$, $a, b \in \mathbb{Z}$.

- 1) We begin by proving that $\pi \equiv 1 \pmod{2+2i}$ (see Chapter 11, Section 5).

For all $t \in \mathbb{F}_p^*$, $\rho(t) = \pm 1$, so $\rho(t) - 1 \equiv 0 \pmod{2}$.

Let's verify that $\chi(t) - 1 \equiv 0 \pmod{1+i}$. $\chi(t) \in \{1, -1, i, -i\}$, so $\chi(t) - 1 \in \{0, -2, i-1, -i-1\}$. As $2 = (1-i)(1+i)$ and $i-1 = i(1+i)$, we obtain

$$\forall t \in \mathbb{F}_p^*, 1+i \mid \chi(t) - 1.$$

Thus

$$\forall s \in \mathbb{F}_p^*, \forall t \in \mathbb{F}_p^*, (\rho(s) - 1)(\chi(t) - 1) \equiv 0 \pmod{2+2i}.$$

Moreover, if $s = 0, t = 1$, then $\chi(t) = 1$, and if $s = 1, t = 0$, then $\rho(s) = 1$, therefore

$$\sum_{s+t=1} (\rho(s) - 1)(\chi(t) - 1) \equiv 0 \pmod{2+2i}.$$

This gives, when developing this expression, :

$$-\pi - \sum_{t \in \mathbb{F}_p} \chi(t) - \sum_{s \in \mathbb{F}_p} \rho(s) + p \equiv 0 \pmod{2+2i}.$$

As $\sum_t \chi(t) = \sum_s \rho(s) = 0$, we obtain

$$\pi \equiv p \pmod{2+2i}.$$

Finally, $p \equiv 1 \pmod{4}$, and $2+2i \mid 4$, since $4 = (1-i)(2+2i)$, thus $p \equiv 1 \pmod{2+2i}$, and

$$\pi \equiv 1 \pmod{2+2i}.$$

2) By Corollary of Theorem 1, $N(\pi) = N(J(\chi, \rho)) = p = a^2 + b^2$.

We know that $p \equiv 1 \pmod{4}$, $p = a^2 + b^2$ and $a + ib \equiv 1 \pmod{2+2i}$. Then we prove that a is odd, b is even, and $a \equiv 1 \pmod{4}$ if $4 \mid b$ and $a \equiv -1 \pmod{4}$ if $4 \nmid b$.

$a + bi \equiv 1 \pmod{2+2i}$, thus $a + bi \equiv 1 \pmod{2}$, so that a is odd, and b is even.

• If $4 \mid b$, then $2+2i \mid b$.

Therefore $a \equiv 1 \pmod{2+2i}$, and by complex conjugation, $a \equiv 1 \pmod{2-2i}$, so $(2+2i)(2-2i) = 8 \mid (a-1)^2$, thus $4 \mid a-1$.

• If $4 \nmid b$, then $b = 4k + 2, k \in \mathbb{Z}$.

Therefore, $1 \equiv a + bi \equiv a + 2i \pmod{2+2i}$. As $2i \equiv -2 \pmod{2+2i}$, $a \equiv 3 \equiv -1 \pmod{2+2i}$. By conjugation, $a \equiv -1 \pmod{2-2i}$. Multiplying these congruences, we obtain $8 \mid (a+1)^2$, thus $a \equiv -1 \pmod{4}$.

3) $\pi = -J(\chi, \rho) = a + bi$ is such that $a^2 + b^2 = p$, a odd, b even and also

$$(4 \mid b \text{ and } a \equiv 1 \pmod{4}) \text{ or } (4 \nmid b \text{ and } a \equiv -1 \pmod{4}).$$

If $p = A^2 + B^2$, A odd and B even, then also $p = (-A)^2 + B^2$, and $A \equiv 1 \pmod{4}$ or $-A \equiv 1 \pmod{4}$. So there exists a decomposition $p = A^2 + B^2$ such that $A \equiv 1 \pmod{4}$, and A is uniquely determined (Ex. 12).

Let's verify that $4 \mid b$ if $p \equiv 1 \pmod{8}$, $4 \nmid b$ if $p \equiv 5 \pmod{8}$.

$$p = a^2 + b^2, a = 2a' + 1, b = 2b', \text{ so } p = 4a'^2 + 4a' + 1 + 4b'^2 = 8\frac{a'(a'+1)}{2} + 1 + 4b'^2.$$

$$\text{Hence } 4 \mid b \iff 2 \mid b' \iff 8 \mid p - 1.$$

Therefore if $p \equiv 1 \pmod{8}$, $\text{Re } \pi = a = A$, and if $p \equiv 5 \pmod{8}$, $\text{Re } \pi = a = -A$.

In conclusion, by Exercise 8.17 :

if $p = A^2 + B^2, A \equiv 1 \pmod{4}$, and $N = N(x^4 + y^4 = 1)$ in \mathbb{F}_p ,

- (a) $N = p - 3 - 6A$ if $p \equiv 1 \pmod{8}$,
(b) $N = p + 1 + 2A$ if $p \equiv 5 \pmod{8}$.

Note : if $p \equiv -1 \pmod{4}$, then there is no character of order 4 on \mathbb{F}_p^* , and $d = 4 \wedge (p - 1) = 4 \wedge (4k + 2) = 2$. By Exercise 1, we obtain

$$N(x^4 = a) = \sum_{\chi^2=1} \chi(a) = 1 + \rho(a) = N(x^2 = a).$$

$$\begin{aligned} N(x^4 + y^4 = 1) &= \sum_{a+b=1} N(x^4 = a)N(y^4 = b) \\ &= \sum_{a+b=1} N(x^2 = a)N(y^2 = b) \\ &= N(x^2 + y^2 = 1). \end{aligned}$$

Using Chapter 8, Section 3, we obtain

$$N(x^4 + y^4 = 1) = p + 1 \text{ if } p \equiv -1 \pmod{4}.$$

□

Ex. 8.19 Find a formula for the number of solutions to $x_1^2 + x_2^2 + \cdots + x_r^2 = 0$ in \mathbb{F}_p .

Proof. Let χ be the Legendre character. Then

$$\begin{aligned} N(x_1^2 + x_2^2 + \cdots + x_r^2 = 0) &= \sum_{a_1+a_2+\cdots+a_r=0} N(x_1^2 = a_1)N(x_2^2 = a_2) \cdots N(x_r^2 = a_r) \\ &= \sum_{a_1+a_2+\cdots+a_r=0} (1 + \chi(a_1))(1 + \chi(a_2)) \cdots (1 + \chi(a_r)) \\ &= p^{r-1} + J_0(\chi, \chi, \dots, \chi) \end{aligned}$$

(We used Proposition 8.5.1). For all k , $\chi^{2k} = \varepsilon$, $\chi^{2k+1} = \chi$.

- If r is odd, $\chi^r \neq \varepsilon$, so $J_0(\chi, \chi, \dots, \chi) = 0$ (Proposition 8.5.1).

$$N(x_1^2 + x_2^2 + \cdots + x_r^2 = 0) = p^{r-1}.$$

- If r is even, $\chi^r = \varepsilon$, so $J_0(\chi, \chi, \dots, \chi) = \chi(-1)(p-1)J(\chi, \chi, \dots, \chi)$, where there are $r-1$ components in the Jacobi sum (Proposition 8.5.1).

By Theorem 3, $J(\chi, \chi, \dots, \chi)g(\chi^{r-1}) = g(\chi)^{r-1}$, and $g(\chi^{r-1}) = g(\chi)$, so

$$J(\chi, \chi, \dots, \chi) = g(\chi)^{r-2}.$$

$g(\chi)^2 = \chi(-1)p$, therefore $\chi^{r-2} = \chi(-1)^{(r/2)-1}p^{(r/2)-1} = (-1)^{((p-1)/2)(r/2-1)}p^{(r/2)-1}$.
So

$$N(x_1^2 + x_2^2 + \cdots + x_r^2 = 0) = p^{r-1} + (-1)^{\frac{p-1}{2} \frac{r}{2}} (p-1)p^{\frac{r}{2}-1}.$$

(Verified in C++ with small values of p and r .)

Conclusion :

$$\begin{cases} N(x_1^2 + x_2^2 + \cdots + x_r^2 = 0) &= p^{r-1} & \text{if } r \text{ is odd,} \\ &= p^{r-1} + (-1)^{\frac{p-1}{2} \frac{r}{2}} (p-1)p^{\frac{r}{2}-1} & \text{if } r \text{ is even.} \end{cases}$$

□

Ex. 8.20 Generalize Proposition 8.6.1 by finding an explicit formula for the number of solutions to $a_1x_1^2 + a_2x_2^2 + \cdots + a_rx_r^2 = 1$ in \mathbb{F}_p .

Proof. Write χ the Legendre character.

$$\begin{aligned} N(a_1x_1^2 + \cdots + a_rx_r^2 = 1) &= \sum_{a_1u_1 + \cdots + a_ru_r = 1} N(x_1^2 = u_1) \cdots N(x_r^2 = u_r) \\ &= \sum_{a_1u_1 + \cdots + a_ru_r = 1} (1 + \chi(u_1)) \cdots (1 + \chi(u_r)) \quad (v_i = a_iu_i) \\ &= \sum_{v_1 + \cdots + v_r = 1} (1 + \chi(a_1)^{-1}\chi(v_1)) \cdots (1 + \chi(a_r)^{-1}\chi(v_r)) \\ &= p^{r-1} + \chi(a_1^{-1}) \cdots \chi(a_r^{-1}) J(\chi, \chi, \dots, \chi). \end{aligned}$$

$$\chi(a_i^{-1}) = \overline{\chi(a_i)} = \chi(a_i) = \left(\frac{a_i}{p}\right).$$

$J(\chi, \chi, \dots, \chi)$ is computed in Chapter 5 Section 6. We obtain

$$\begin{cases} N(a_1x_1^2 + \cdots + a_rx_r^2 = 1) &= p^{r-1} + \left(\frac{a_1}{p}\right) \cdots \left(\frac{a_r}{p}\right) (-1)^{\frac{r-1}{2} \frac{p-1}{2}} p^{\frac{r-1}{2}} & \text{if } r \text{ is odd,} \\ &= p^{r-1} - \left(\frac{a_1}{p}\right) \cdots \left(\frac{a_r}{p}\right) (-1)^{\frac{r}{2} \frac{p-1}{2}} p^{\frac{r}{2}-1} & \text{if } r \text{ is even.} \end{cases}$$

□

Ex. 8.21 Suppose that $p \equiv 1 \pmod{d}$, $\zeta = e^{2\pi i/p}$, and consider $\sum_x \zeta^{ax^d}$. Show that $\sum_x \zeta^{ax^d} = \sum_r m(r) \zeta^{ar}$, where $m(r) = N(x^d = r)$.

Proof. Let $A_r = \{x \in \mathbb{F}_p \mid x^d = r\}$

Then $\mathbb{F}_p = \coprod_r A_r$, thus

$$\sum_{x \in \mathbb{F}_p} \zeta^{ax^d} = \sum_{r \in \mathbb{F}_p} \sum_{x \in A_r} \zeta^{ax^d} = \sum_{r \in \mathbb{F}_p} |A_r| \zeta^{ar} = \sum_{r \in \mathbb{F}_p} m(r) \zeta^{ar},$$

where $m(r) = |A_r| = N(x^d = r)$.

□

Ex. 8.22 (continuation) Prove that $\sum_x \zeta^{ax^d} = \sum_{\chi} g_a(\chi)$, where the sum is over all χ such that $\chi^d = \varepsilon$, $\chi \neq \varepsilon$. Assume that $p \nmid a$.

Proof. By Exercise 8.21,

$$S = \sum_{x \in \mathbb{F}_p} \zeta^{ax^d} = \sum_{r \in \mathbb{F}_p} m(r) \zeta^{ar}.$$

As $d \mid p-1$, by Proposition 8.1.5,

$$m(r) = N(x^d = r) = \sum_{\chi^d = \varepsilon} \chi(r).$$

Therefore

$$S = \sum_{r \in \mathbb{F}_p} \sum_{\chi^d = \varepsilon} \chi(r) \zeta^{ar} = \sum_{\chi^d = \varepsilon} \sum_{r \in \mathbb{F}_p} \chi(r) \zeta^{ar}.$$

If $\chi = \varepsilon$, $\sum_{r \in \mathbb{F}_p} \chi(r) \zeta^{ar} = \sum_{r \in \mathbb{F}_p} \zeta^{ar} = 0$, since $a \not\equiv 0 \pmod{p}$.

By definition $g_a(\chi) = \sum_r \chi(r) \zeta^{ar}$, so, if $d \mid p-1$, $p \nmid a$,

$$\sum_{x \in \mathbb{F}_p} \zeta^{ax^d} = \sum_{\chi^d = \varepsilon, \chi \neq \varepsilon} g_a(\chi).$$

□

Ex. 8.23 Let $f(x_1, x_2, \dots, x_n) \in \mathbb{F}_p[x_1, x_2, \dots, x_n]$. Let N be the number of zeros of f in \mathbb{F}_p . Show that $N = p^{n-1} + p^{-1} \sum_{a \neq 0} (\sum_{x_1, \dots, x_n} \zeta^{af(x_1, \dots, x_n)})$.

Proof. Let $A_r = \{(x_1, x_2, \dots, x_n) \in \mathbb{F}_p^n \mid f(x_1, x_2, \dots, x_n) = r\}$. Then $\mathbb{F}_p^n = \coprod_{r \in \mathbb{F}_p} A_r$, so, for all $a \in \mathbb{F}_p$,

$$\begin{aligned} \sum_{(x_1, x_2, \dots, x_n) \in \mathbb{F}_p^n} \zeta^{af(x_1, x_2, \dots, x_n)} &= \sum_{r \in \mathbb{F}_p} \sum_{(x_1, x_2, \dots, x_n) \in A_r} \zeta^{ar} \\ &= \sum_{r \in \mathbb{F}_p} |A_r| \zeta^{ar}. \end{aligned}$$

Let $m(r) = |A_r| = N(f(x_1, x_2, \dots, x_n) = r)$. Then

$$\begin{aligned} \sum_{a \in \mathbb{F}_p} \sum_{(x_1, x_2, \dots, x_n) \in \mathbb{F}_p^n} \zeta^{af(x_1, x_2, \dots, x_n)} &= \sum_{a \in \mathbb{F}_p} \sum_{r \in \mathbb{F}_p} m(r) \zeta^{ar} \\ &= \sum_{r \in \mathbb{F}_p} m(r) \sum_{a \in \mathbb{F}_p} \zeta^{ar} \end{aligned}$$

As $\sum_{a \in \mathbb{F}_p} \zeta^{ar} = 0$ if $r \neq 0$, and $\sum_{a \in \mathbb{F}_p} \zeta^{ar} = p$ if $r = 0$, we obtain

$$\sum_{a \in \mathbb{F}_p} \sum_{(x_1, x_2, \dots, x_n) \in \mathbb{F}_p^n} \zeta^{af(x_1, x_2, \dots, x_n)} = m(0)p = pN.$$

Moreover

$$\sum_{a \in \mathbb{F}_p} \sum_{(x_1, x_2, \dots, x_n) \in \mathbb{F}_p^n} \zeta^{af(x_1, x_2, \dots, x_n)} = p^n + \sum_{a \in \mathbb{F}_p^*} \sum_{(x_1, x_2, \dots, x_n) \in \mathbb{F}_p^n} \zeta^{af(x_1, x_2, \dots, x_n)},$$

so

$$pN = p^n + \sum_{a \in \mathbb{F}_p^*} \sum_{(x_1, x_2, \dots, x_n) \in \mathbb{F}_p^n} \zeta^{af(x_1, x_2, \dots, x_n)}.$$

In conclusion,

$$N = p^{n-1} + p^{-1} \sum_{a \in \mathbb{F}_p^*} \sum_{(x_1, x_2, \dots, x_n) \in \mathbb{F}_p^n} \zeta^{af(x_1, x_2, \dots, x_n)}.$$

□

Ex. 8.24 (continuation) Let $f(x_1, x_2, \dots, x_n) = a_1 x_1^{m_1} + a_2 x_2^{m_2} + \dots + a_n x_n^{m_n}$. Let $d_i = (m_i, p-1)$. Show that $N = p^{n-1} + p^{-1} \sum_{a \neq 0} \prod_{i=1}^n \sum_{\chi_i} g_{aa_i}(\chi_i)$ where χ_i runs over all characters such that $\chi_i^{d_i} = \varepsilon$ and $\chi_i \neq \varepsilon$.

Proof. By Exercise 8.2,

$$N = N(a_1 x_1^{m_1} + \dots + a_n x_n^{m_n} = 0) = N(a_1 x_1^{d_1} + \dots + a_n x_n^{d_n} = 0),$$

where $d_i = m_i \wedge (p-1)$ divides $p-1$.

By Exercise 8.23,

$$N = p^{n-1} + p^{-1} \sum_{a \in \mathbb{F}_p^*} \sum_{(x_1, x_2, \dots, x_n) \in \mathbb{F}_p^n} \zeta^{a(a_1 x_1^{d_1} + \dots + a_n x_n^{d_n})}$$

By Exercise 8.22, since $p \nmid a, p \nmid a_i$,

$$\begin{aligned} \sum_{(x_1, x_2, \dots, x_n) \in \mathbb{F}_p^n} \zeta^{a(a_1 x_1^{d_1} + \dots + a_n x_n^{d_n})} &= \left(\sum_{x_1 \in \mathbb{F}_p} \zeta^{a a_1 x_1^{d_1}} \right) \dots \left(\sum_{x_n \in \mathbb{F}_p} \zeta^{a a_n x_n^{d_n}} \right) \\ &= \left(\sum_{\chi_1^{d_1} = \varepsilon, \chi_1 \neq \varepsilon} g_{a a_1}(\chi_1) \right) \dots \left(\sum_{\chi_n^{d_n} = \varepsilon, \chi_n \neq \varepsilon} g_{a a_n}(\chi_n) \right) \\ &= \prod_{i=1}^n \sum_{\chi_i^{d_i} = \varepsilon, \chi_i \neq \varepsilon} g_{a a_i}(\chi_i) \end{aligned}$$

In conclusion,

$$N = p^{n-1} + p^{-1} \sum_{a \in \mathbb{F}_p^*} \prod_{i=1}^n \sum_{\chi_i^{d_i} = \varepsilon, \chi_i \neq \varepsilon} g_{a a_i}(\chi_i).$$

□

Ex. 8.25 Deduce from Exercise 8.24 that

$$|N - p^{n-1}| \leq (p-1)(d_1-1) \dots (d_n-1) p^{(n/2)-1}.$$

Proof. As $|g_{a a_i}(\chi_i)| = \sqrt{p}$,

$$\left| \sum_{\chi_i^{d_i} = \varepsilon, \chi_i \neq \varepsilon} g_{a a_i}(\chi_i) \right| \leq \sqrt{p} n_i,$$

where $n_i = \text{Card} \{ \chi_i \neq \varepsilon \mid \chi_i^{d_i} = \varepsilon \}$.

As $d_i \mid p-1$, there exists exactly d_i characters of order dividing d_i , so $n_i = d_i - 1$:

$$\left| \sum_{\chi_i^{d_i} = \varepsilon, \chi_i \neq \varepsilon} g_{a a_i}(\chi_i) \right| \leq \sqrt{p}(d_i - 1).$$

By Exercise 8.24,

$$N = p^{n-1} + p^{-1} \sum_{a \in \mathbb{F}_p^*} \prod_{i=1}^n \sum_{\chi_i^{d_i} = \varepsilon, \chi_i \neq \varepsilon} g_{a a_i}(\chi_i)$$

so

$$|N - p^{n-1}| \leq p^{-1}(p-1)\sqrt{p}(d_1-1) \dots \sqrt{p}(d_n-1),$$

that is

$$|N - p^{n-1}| \leq (p-1)(d_1-1) \dots (d_n-1) p^{\frac{n}{2}-1}.$$

□

Ex. 8.26 Let p be a prime, $p \equiv 1 \pmod{4}$, χ a multiplicative character of order 4 on \mathbb{F}_p , and ρ the Legendre symbol. Put $J(\chi, \rho) = a + bi$. Show

(a) $N(y^2 + x^4 = 1) = p - 1 + 2a$.

(b) $N(y^2 = 1 - x^4) = p + \sum \rho(1 - x^4)$.

(c) $2a \equiv -(-1)^{(p-1)/4} \binom{2m}{m} \pmod{p}$ where $m = (p-1)/4$.

(d) Verify (c) for $p = 13, 17, 29$.

Proof. (a) By Proposition 8.1.5,

$$\begin{aligned} N(y^2 + x^4 = 1) &= \sum_{a+b=1} N(y^2 = a)N(x^4 = b) \\ &= \sum_{a+b=1} (1 + \rho(a))(1 + \chi(b) + \chi^2(b) + \chi^3(b)) \\ &= \sum_{i=0}^1 \sum_{j=0}^3 \sum_{a+b=1} \rho^i(a) \chi^j(b) \\ &= \sum_{i=0}^1 \sum_{j=0}^3 J(\rho^i, \chi^j) \end{aligned}$$

As $J(\varepsilon, \varepsilon) = p$, and $0 = J(\varepsilon, \chi) = J(\varepsilon, \chi^2) = J(\varepsilon, \chi^3) = J(\rho, \varepsilon)$, we obtain

$$N(y^2 + x^4 = 1) = p + J(\rho, \chi) + J(\rho, \chi^2) + J(\rho, \chi^3).$$

As $J(\rho, \chi^3) = J(\bar{\rho}, \bar{\chi}) = \overline{J(\rho, \chi)}$, and $J(\rho, \chi^2) = J(\rho, \rho) = J(\rho, \rho^{-1}) = -\rho(-1) = -(-1)^{(p-1)/2} = -1$ (since $p \equiv 1 \pmod{4}$). Moreover, by Exercise 8.7,

$$J(\chi, \rho) = \chi(-1)J(\chi, \chi) = \pm J(\chi, \chi) \in \mathbb{Z}[i] : J(\chi, \rho) = a + bi, (a, b) \in \mathbb{Z}^2.$$

Thus $N(y^2 + x^4 = 1) = p + 2 \operatorname{Re} J(\chi, \rho) + J(\rho, \rho) = p - 1 + 2a$

In conclusion,

$$N(y^2 + x^4 = 1) = p - 1 + 2a, \text{ where } J(\chi, \rho) = a + bi.$$

(b) By Exercise 8.8,

$$\begin{aligned} \sum_{t \in \mathbb{F}_p} \rho(1 - t^4) &= \sum_{\lambda^4 = \varepsilon} J(\rho, \lambda) \\ &= J(\rho, \varepsilon) + J(\rho, \chi) + J(\rho, \chi^2) + J(\rho, \chi^3) \\ &= J(\rho, \rho) + J(\rho, \chi) + J(\rho, \bar{\chi}) \\ &= -1 + 2 \operatorname{Re} J(\chi, \rho) \\ &= -1 + 2a \end{aligned}$$

So $N(y^2 = 1 - x^4) = p - 1 + 2a = p + \sum_{t \in \mathbb{F}_p} \rho(1 - t^4)$.

(c) Reducing modulo p , and writing $\bar{a} \in \mathbb{F}_p$ the class of a , we obtain :

$$\begin{aligned}
2\bar{a} &= 1 + \sum_{t \in \mathbb{F}_p} \rho(1 - t^4) \\
&= 1 + \sum_{t \in \mathbb{F}_p} (1 - t^4)^{\frac{p-1}{2}} \\
&= 1 + \sum_{t \in \mathbb{F}_p} \sum_{k=0}^{(p-1)/2} \binom{\frac{p-1}{2}}{k} (-1)^k t^{4k} \\
&= 1 + \sum_{k=0}^{(p-1)/2} (-1)^k \binom{\frac{p-1}{2}}{k} \sum_{t \in \mathbb{F}_p} t^{4k} \\
&= 1 + \sum_{k=1}^{(p-1)/2} (-1)^k \binom{\frac{p-1}{2}}{k} \sum_{t \in \mathbb{F}_p^*} t^{4k}.
\end{aligned}$$

Let $S_k = \sum_{t \in \mathbb{F}_p^*} t^{4k}$, $k > 0$, and g a generator of \mathbb{F}_p^* : $t = g^i, 0 \leq i \leq p-2$.

$$S_k = \sum_{i=0}^{p-2} (g^i)^{4k} = \sum_{i=0}^{p-2} (g^{4k})^i.$$

If $g^{4k} \neq 1$, $S_k \equiv \frac{g^{4k(p-1)} - 1}{g^{4k} - 1} = 0$, if not $S_k = p - 1 = -1$.

For every k , $1 \leq k \leq (p-1)/2$,

$$g^{4k} = 1 \iff p-1 \mid 4k \iff \frac{p-1}{4} \mid k \iff k = \frac{p-1}{4} \text{ or } k = \frac{p-1}{2},$$

therefore

$$2a \equiv 1 - (-1)^{\frac{p-1}{4}} \binom{\frac{p-1}{2}}{\frac{p-1}{4}} - (-1)^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{\frac{p-1}{2}} \pmod{p},$$

$$2a \equiv -(-1)^{\frac{p-1}{4}} \binom{\frac{p-1}{2}}{\frac{p-1}{4}} \pmod{p}.$$

(d) • If $p = 13$, I choose the primitive root $g = \bar{2}$, and χ the character of order 4 defined by $\chi(g) = i$ (the only other character of order 4 is $\bar{\chi}$).

Then $J(\chi, \rho) = -3 + 2i, a = -3$.

$$N = p - 1 + 2a = 6.$$

$$2a = -6, -(-1)^{\frac{13-1}{4}} \binom{6}{3} = 20 \text{ et } -6 \equiv 20 \pmod{13}.$$

• If $p = 17$, $g = 3$, $\chi(g) = i$, $J(\chi, \rho) = -1 + 4i, a = -1$.

$$N = p - 1 + 2a = 14.$$

$$2a = -2, -(-1)^{\frac{17-1}{4}} \binom{8}{4} = -70 \equiv -2 \pmod{17}.$$

- Si $p = 29$, $g = 3$, $\chi(g) = i$, $J(\chi, \rho) = 5 + 2i$, $a = 5$.

$$N = p - 1 + 2a = 38.$$

$$2a = 10, -(-1)^{\frac{29-1}{4}} \binom{14}{7} = 3432 \equiv 10 \pmod{29} \quad (3422 = 118 \times 29).$$

Note : By Prop. 8.3.1 (and Ex. 8.7), $p = |J(\chi, \rho)|^2 = |J(\chi, \chi)|^2$, so $a^2 + b^2 = p$ (where $p = 4m + 1$).

As $\binom{2m}{m} = 2\binom{2m-1}{m-1}$ is even, and as p is an odd prime $a \equiv \pm \frac{1}{2} \binom{2m}{m} \pmod{p}$.

Since $p \geq 5$, $p = a^2 + b^2$ implies $|a| < \sqrt{p} < p/2$, thus the least remainder of $\frac{1}{2} \binom{2m}{m}$ is $\pm a$.

Moreover, from Wilson theorem, we obtain a square root of -1 in \mathbb{F}_p ($p = 4m + 1$) :

$$-1 \equiv (p-1)! \equiv \left[(-1)^{(p-1)/4} \left(\frac{p-1}{2} \right)! \right]^2 = [(2m)!]^2.$$

Since $(\bar{b}a^{-1})^2 = -1$ in \mathbb{F}_p , we obtain $b \equiv (2m)!a \pmod{p}$. The conclusion is the proposition of Gauss, which gives an explicit formula for the solution of $p = a^2 + b^2$:

Proposition Let p a prime of the form $p = 4m + 1$.

If

$$\begin{aligned} a &\equiv \frac{1}{2} \binom{2m}{m} \pmod{p}, & -\frac{p}{2} < a < \frac{p}{2}, \\ b &\equiv (2m)!a \pmod{p}, & -\frac{p}{2} < b < \frac{p}{2}, \end{aligned}$$

then $p = a^2 + b^2$. □

Ex. 8.27 Let $p \equiv 1 \pmod{3}$, χ a character of order 3, ρ the Legendre symbol. Show

- (a) $N(y^2 = 1 - x^3) = p + \sum \rho(1 - x^3)$.
- (b) $N(y^2 + x^3 = 1) = p + 2 \operatorname{Re} J(\chi, \rho)$.
- (c) $2a - b \equiv -\binom{(p-1)/2}{(p-1)/3} \pmod{p}$ where $J(\chi, \rho) = a + b\omega$.

Proof. (b) By Exercise 8.15,

$$N(y^2 = x^3 + D) = p + 2 \operatorname{Re} (\pi), \text{ where } \pi = (\rho\chi)(D)J(\chi, \rho).$$

Moreover, with $D = 1$, we obtain

$$\begin{aligned} N(y^2 + x^3 = 1) &= N(y^2 + (-x)^3 = 1) \\ &= p + 2 \operatorname{Re} J(\chi, \rho). \end{aligned}$$

$$J(\chi, \rho) = \sum_{a+b=1} \chi(a)\rho(b), \text{ where } \rho(b) \in \{-1, 1\}, \chi(a) \in \{1, \omega, \omega^2\}, \text{ so } J(\chi, \rho) \in \mathbb{Z}[\omega].$$

$$J(\chi, \rho) = a + b\omega, a \in \mathbb{Z}, b \in \mathbb{Z} \text{ and } 2 \operatorname{Re} (J(\chi, \rho)) = 2a - b.$$

(a) By Exercise 8.8,

$$\begin{aligned}\sum_x \rho(1-x^3) &= \sum_{\lambda^3=\varepsilon} J(\rho, \lambda) \\ &= J(\rho, \varepsilon) + J(\rho, \chi) + J(\rho, \chi^2) \\ &= 2 \operatorname{Re} J(\chi, \rho).\end{aligned}$$

So

$$\begin{aligned}N(y^2 = 1 - x^3) &= p + \sum_x \rho(1 - x^3) \\ &= p + 2a - b.\end{aligned}$$

(c) Reducing modulo p , we obtain in \mathbb{F}_p :

$$\begin{aligned}2\bar{a} - \bar{b} &= \sum_x \rho(1 - x^3) \\ &= \sum_{t \in \mathbb{F}_p} (1 - t^3)^{\frac{p-1}{2}} \\ &= \sum_{t \in \mathbb{F}_p} \sum_{k=0}^{(p-1)/2} \binom{\frac{p-1}{2}}{k} (-1)^k t^{3k} \\ &= \sum_{k=0}^{(p-1)/2} (-1)^k \binom{\frac{p-1}{2}}{k} \sum_{t \in \mathbb{F}_p} t^{3k} \\ &= \sum_{k=1}^{(p-1)/2} (-1)^k \binom{\frac{p-1}{2}}{k} \sum_{t \in \mathbb{F}_p} t^{3k}.\end{aligned}$$

Let $S_k = \sum_{t \in \mathbb{F}_p} t^{3k}$ ($0 < k \leq \frac{p-1}{2}$), and g a primitive root in \mathbb{F}_p : $t = g^i, 0 \leq i \leq p-2$.

$$S_k = \sum_{i=0}^{p-2} (g^i)^{3k} = \sum_{i=0}^{p-2} (g^{3k})^i$$

If $g^{3k} \neq 1$, $S_k = \frac{g^{3k(p-1)} - 1}{g^{3k} - 1} = 0$, if not $S_k = p - 1 = -1$.

$$g^{3k} = 1 \iff p-1 \mid 3k \iff \frac{p-1}{3} \mid k \iff k = \frac{p-1}{3}$$

and $\frac{p-1}{3}$ even, so

$$2a - b \equiv -\binom{\frac{p-1}{2}}{\frac{p-1}{3}} \pmod{p} \quad (\text{where } J(\chi, \rho) = a + b\omega).$$

□

Ex. 8.28 Let $p \equiv 3 \pmod{4}$ and χ the quadratic character defined on $\mathbb{Z}/p\mathbb{Z}$. Show

$$(a) \sum_{x=1}^{p-1} x\chi(x) = 2 \sum_{x=1}^{(p-1)/2} x\chi(x) - p \sum_{x=1}^{(p-1)/2} \chi(x).$$

$$(b) \sum_{x=1}^{p-1} x\chi(x) = 4\chi(2) \sum_{x=1}^{(p-1)/2} x\chi(x) - p\chi(2) \sum_{x=1}^{(p-1)/2} \chi(x).$$

(c) If $p \equiv 3 \pmod{8}$ then $\sum_{x=1}^{p-1} x\chi(x)/p = -\frac{1}{3} \sum_{x=1}^{(p-1)/2} \chi(x)$.

(d) If $p \equiv 7 \pmod{8}$ then $\sum_{x=1}^{p-1} x\chi(x)/p = -\sum_{x=1}^{(p-1)/2} \chi(x)$.

Note : I added two minus signs in (c) and (d) to write a true sentence. See the verification below.

Proof. (a) $\chi(-1) = (-1)^{(p-1)/2} = -1$, and $\chi(p-x) = \chi(-x) = \chi(-1)\chi(x) = -\chi(x)$, thus

$$\begin{aligned} \sum_{x=1}^{p-1} x\chi(x) &= \sum_{x=1}^{(p-1)/2} x\chi(x) + \sum_{x=(p-1)/2+1}^{p-1} x\chi(x) \\ &= \sum_{x=1}^{(p-1)/2} x\chi(x) + \sum_{y=1}^{(p-1)/2} (p-y)\chi(p-y) \quad (x = p-y) \\ &= \sum_{x=1}^{(p-1)/2} x\chi(x) - \left[p \sum_{x=1}^{(p-1)/2} \chi(x) - \sum_{x=1}^{(p-1)/2} x\chi(x) \right] \\ &= 2 \sum_{x=1}^{(p-1)/2} x\chi(x) - p \sum_{x=1}^{(p-1)/2} \chi(x). \end{aligned}$$

(b) If we separate even and odd indices, we obtain, as p is odd :

$$\begin{aligned} \sum_{x=1}^{p-1} x\chi(x) &= \sum_{k=1}^{(p-1)/2} 2k\chi(2k) + \sum_{k=0}^{(p-1)/2-1} (2k+1)\chi(2k+1) \\ &= \sum_{x=1}^{(p-1)/2} 2x\chi(2x) + \sum_{x=1}^{(p-1)/2} (p-2x)\chi(p-2x) \quad (2k+1 = p-2x) \\ &= 2\chi(2) \sum_{x=1}^{(p-1)/2} x\chi(x) - \chi(2) \sum_{x=1}^{(p-1)/2} (p-2x)\chi(x) \\ &= 4\chi(2) \sum_{x=1}^{(p-1)/2} x\chi(x) - p\chi(2) \sum_{x=1}^{(p-1)/2} \chi(x). \end{aligned}$$

(c) Let $S = \sum_{x=1}^{(p-1)/2} \chi(x)$, $T = \sum_{x=1}^{(p-1)/2} x\chi(x)$. Then

$$\begin{aligned} (a) \sum_{x=1}^{p-1} x\chi(x) &= 2T - pS, \\ (b) \sum_{x=1}^{p-1} x\chi(x) &= 4\chi(2)T - p\chi(2)S. \end{aligned}$$

Subtracting these equalities, we obtain

$$\begin{aligned} (4\chi(2) - 2)T &= p(\chi(2) - 1)S, \\ \frac{T}{p} &= \frac{\chi(2) - 1}{4\chi(2) - 2}S. \end{aligned}$$

$\chi(2) = (-1)^{(p^2-1)/8} = -1$ if $p \equiv 3 \pmod{8}$, so $\frac{\chi(2)-1}{4\chi(2)-2} = \frac{1}{3}$, and $T/p = (1/3)S$.

$$\sum_{x=1}^{p-1} x\chi(x)/p = 2T/p - S = -(1/3)S,$$

$$\sum_{x=1}^{p-1} x\chi(x)/p = -\frac{1}{3} \sum_{x=1}^{(p-1)/2} \chi(x).$$

(d) $\chi(2) = (-1)^{(p^2-1)/8} = 1$ if $p \equiv 7 \pmod{8}$: $\frac{\chi(2)-1}{4\chi(2)-2} = 0$.

$$\sum_{x=1}^{p-1} x\chi(x)/p = - \sum_{x=1}^{(p-1)/2} \chi(x).$$

Verification : with $p = 7$, the squares are 1, 4, 2 = 9, so

$$\begin{aligned} \sum_{x=1}^{p-1} x\chi(x)/p &= \frac{1}{7} \left[\left(\frac{1}{7}\right) + 2\left(\frac{2}{7}\right) + 3\left(\frac{3}{7}\right) + 4\left(\frac{4}{7}\right) + 5\left(\frac{5}{7}\right) + 6\left(\frac{6}{7}\right) \right] \\ &= \frac{1}{7} (1 + 2 - 3 + 4 - 5 - 6) = -1 \\ \sum_{x=1}^{(p-1)/2} \chi(x) &= \left(\frac{1}{7}\right) + \left(\frac{2}{7}\right) + \left(\frac{3}{7}\right) \\ &= 1 + 1 - 1 = 1. \end{aligned}$$

With $p = 3$,

$$\begin{aligned} \sum_{x=1}^{p-1} x\chi(x)/p &= \frac{1}{3} \left[\left(\frac{1}{3}\right) + 2\left(\frac{2}{3}\right) \right] \\ &= \frac{1}{3} (1 - 2) = -\frac{1}{3} \\ \sum_{x=1}^{(p-1)/2} \chi(x) &= \left(\frac{1}{3}\right) \\ &= 1 \end{aligned}$$

This confirms the misprints in the initial sentence. □