

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

Richard Ganaye

August 21, 2022

Chapter 4

Ex. 4.1 *Show that 2 is a primitive root modulo 29.*

Proof. Let $p = 29 : p - 1 = 2^2 \times 7$.

$$2^4 = 16 \not\equiv 1 [29]$$

$$2^{14} = 4^7 = 4 \times 16^3 = 64 \times 256 \equiv 6 \times (-34) = -204 \equiv 86 = 3 \times 29 - 1 \equiv -1 [29]$$

$$2^{28} \equiv 1 [29] \text{ and } 2^d \not\equiv 1 \text{ if } d \mid 28, d < 28, \text{ hence 2 is a primitive element modulo 29. } \square$$

Ex. 4.2 *Compute all primitive roots for $p = 11, 13, 17$, and 19.*

Proof. • $p = 11$. Then $p - 1 = 10 = 2 \times 5$.

$2^2 = 4 \not\equiv 1 \pmod{11}$, and $2^5 = 32 \equiv -1 \not\equiv 1 \pmod{11}$, so 2 is a primitive element modulo 11.

The other primitive elements modulo 11 are congruent to the powers $2^i, i \wedge 10 = 1, 1 \leq i < 10$, namely $2, 2^3, 2^7, 2^9$.

$$2^7 \equiv 7 \pmod{11}, 2^9 \equiv 6 \pmod{11}, \text{ so}$$

$$\{\bar{2}, \bar{8}, \bar{7}, \bar{6}\} \text{ is the set of the generators of } U(\mathbb{Z}/11\mathbb{Z}).$$

Similarly :

$$\bullet p = 13 : \{2, 6, 11, 7\} \text{ is the set of the generators of } U(\mathbb{Z}/13\mathbb{Z}).$$

$$\bullet p = 17 : \{3, 10, 5, 11, 14, 7, 12, 6\} \text{ is the set of the generators of } U(\mathbb{Z}/17\mathbb{Z}).$$

$$\bullet p = 19 : \{2, 13, 14, 15, 3, 10\} \text{ is the set of the generators of } U(\mathbb{Z}/19\mathbb{Z}).$$

I obtain these results with the direct orders in S.A.G.E. :

```
p = 19; Fp = GF(p); a = Fp.multiplicative_generator()
print([a^k for k in range(1,p) if gcd(k,p-1) == 1])
```

□

Ex. 4.3 *Suppose that a is a primitive root modulo p^n , p an odd prime. Show that a is a primitive root modulo p .*

Proof. Suppose that a is a primitive root modulo p^n : then \bar{a} is a generator of $U(\mathbb{Z}/p^n\mathbb{Z})$.

If a was not a primitive root modulo p , \bar{a} is not a generator of $U(\mathbb{Z}/p\mathbb{Z})$, so there exists $b \in \mathbb{Z}, b \wedge p = 1$ such that $a^k \not\equiv b \pmod{p}$ for all $k \in \mathbb{Z}$. A fortiori $a^k \not\equiv b \pmod{p^n}$, and $b \wedge p^n = 1$, so $\bar{b} \in U(\mathbb{Z}/p^n\mathbb{Z})$ and $\bar{b} \notin \langle \bar{a} \rangle$ in $U(\mathbb{Z}/p^n\mathbb{Z})$, in contradiction with the hypothesis. So a is a primitive root modulo p .

(the reasoning on the orders of a , modulo p and modulo p^n , is possible, but not so easy.) □

Ex. 4.4 Consider a prime p of the form $4t + 1$. Show that a is a primitive root modulo p iff $-a$ is a primitive root modulo p .

Proof. Solution 1.

Suppose that a is a primitive root modulo p . As $p - 1$ is even, $(-a)^{p-1} = a^{p-1} \equiv 1 \pmod{p}$.

If $(-a)^n \equiv 1 \pmod{p}$, with $n \in \mathbb{N}$, then $a^n \equiv (-1)^n \pmod{p}$.

Therefore $a^{2n} \equiv 1 \pmod{p}$. As a is a primitive root modulo p , $p - 1 \mid 2n$, $2t \mid n$, so n is even.

Hence $a^n \equiv 1 \pmod{p}$, and $p - 1 \mid n$. So the least $n \in \mathbb{N}^*$ such that $(-a)^n \equiv 1 \pmod{p}$ is $p - 1$: the order of $-a$ modulo p is $p - 1$, $-a$ is a primitive root modulo p .

Conversely, if $-a$ is a primitive root modulo p , we apply the previous result at $-a$ to obtain that $-(-a) = a$ is a primitive root.

Solution 2.

Let $p - 1 = 2^{a_0} p_1^{a_1} \cdots p_k^{a_k}$ the decomposition of $p - 1$ in prime factors.

As p_i is odd for $i = 1, 2, \dots, k$, $(p - 1)/p_i$ is even, and a is primitive, so

$$\begin{aligned} (-a)^{(p-1)/p_i} &= a^{(p-1)/p_i} \not\equiv 1 \pmod{p}, \\ (-a)^{(p-1)/2} &= (-a)^{2k} = a^{2k} = a^{(p-1)/2} \not\equiv 1 \pmod{p}. \end{aligned}$$

So the order of a is $p - 1$ modulo p (see Ex. 4.8): a is a primitive element modulo p . \square

Ex. 4.5 Consider a prime p of the form $4t + 3$. Show that a is a primitive root modulo p iff $-a$ has order $(p - 1)/2$.

Proof. Let a a primitive root modulo p .

As $a^{p-1} \equiv 1 \pmod{p}$, $p \mid (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1)$, so $p \mid a^{(p-1)/2} - 1$ or $p \mid a^{(p-1)/2} + 1$. As a is a primitive root modulo p , $a^{(p-1)/2} \not\equiv 1 \pmod{p}$, so

$$a^{(p-1)/2} \equiv -1 \pmod{p}.$$

Hence $(-a)^{(p-1)/2} = (-1)^{2t+1} a^{(p-1)/2} \equiv (-1) \times (-1) = 1 \pmod{p}$.

Suppose that $(-a)^n \equiv 1 \pmod{p}$, with $n \in \mathbb{N}$.

Then $a^{2n} = (-a)^{2n} \equiv 1 \pmod{p}$, so $p - 1 \mid 2n$, $\frac{p-1}{2} \mid n$.

So $-a$ has order $(p - 1)/2$ modulo p .

Conversely, suppose that $-a$ has order $(p - 1)/2 = 2t + 1$ modulo p . Let $2, p_1, \dots, p_k$ the prime factors of $p - 1$, where p_i are odd.

$a^{(p-1)/2} = a^{2t+1} = -(-a)^{2t+1} = -(-a)^{(p-1)/2} \equiv -1$, so $a^{(p-1)/2} \not\equiv 1 \pmod{p}$.

As $p - 1$ is even, $(p - 1)/p_i$ is even, so

$a^{(p-1)/p_i} = (-a)^{(p-1)/p_i} \not\equiv 1 \pmod{p}$ (since $-a$ has order $p - 1$).

So the order of a is $p - 1$ (see Ex. 4.8): a is a primitive root modulo p . \square

Ex. 4.6 If $p = 2^{2^n} + 1$ is a Fermat prime, show that 3 is a primitive root modulo p .

Proof. Solution 1 (with quadratic reciprocity).

Write $p = 2^k + 1$, with $k = 2^n$.

We suppose that $n > 0$, so $k \geq 2, p \geq 5$. As p is prime, $3^{p-1} \equiv 1 \pmod{p}$.

In other words, $3^{2^k} \equiv 1 \pmod{p}$: the order of 3 is a divisor of 2^k , a power of 2.

3 has order 2^k modulo p iff $3^{2^{k-1}} \not\equiv 1 \pmod{p}$. As $\left(3^{2^{k-1}}\right)^2 \equiv 1 \pmod{p}$, where p is prime, this is equivalent to $3^{2^{k-1}} \equiv -1 \pmod{p}$, which remains to prove.

$$3^{2^{k-1}} = 3^{(p-1)/2} \equiv \left(\frac{3}{p}\right) \pmod{p}.$$

As the result is true for $p = 5$, we can suppose $n \geq 2$. From the law of quadratic reciprocity :

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(p-1)/2} = (-1)^{2^{k-1}} = 1.$$

$$\text{So } \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$$

$$\begin{aligned} p = 2^{2^n} + 1 &\equiv (-1)^{2^n} + 1 \pmod{3} \\ &\equiv 2 \equiv -1 \pmod{3}, \end{aligned}$$

so $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = -1$, that is to say

$$3^{2^{k-1}} \equiv -1 \pmod{p}.$$

The order of 3 modulo $p = 2^{2^n} + 1$ is $p - 1 = 2^{2^n} : 3$ is a primitive root modulo p .
(On the other hand, if 3 is of order $p - 1$ modulo p , then p is prime, so

$$F_n = 2^{2^n} + 1 \text{ is prime} \iff 3^{(F_n-1)/2} = 3^{2^{2^n-1}} \equiv -1 \pmod{F_n}.)$$

Solution 2 (without quadratic reciprocity, with the hint of chapter 4).

As above, if we suppose that 3 is not a primitive root modulo p , then $3^{2^{n-1}} \equiv 1 \pmod{p}$, so $n \geq 2$, and $(-3)^{(p-1)/2} = 3^{2^{n-1}} \equiv 1 \pmod{p}$, so -3 is a square modulo p : there exists $a \in \mathbb{Z}$ such that $-3 \equiv a^2 \pmod{p}$.

As $2 \wedge p = 1$, there exists $u \in \mathbb{Z}$ such that $2u \equiv -1 + a \pmod{p}$ (\bar{u} is similar to $\omega = \frac{-1+i\sqrt{3}}{2} \in \mathbb{C}$). Then

$$\begin{aligned} 8u^3 &\equiv (-1 + a)^3 \\ &\equiv -1 + 3a - 3a^2 + a^3 \\ &\equiv -1 + 3a + 9 - 3a \\ &\equiv 8 \pmod{p} \end{aligned}$$

As $p \wedge 2 = p \wedge 8 = 1$, $u^3 \equiv 1 \pmod{p}$. Moreover, if $u \equiv 1 \pmod{3}$, then $a \equiv 3 \pmod{p}$, $-3 \equiv 9 \pmod{p}$, $p \mid 12$, so $p = 2$ or $p = 3$, in contradiction with $p \geq 5$. So the order of u modulo p is 3 : $(\mathbb{Z}/p\mathbb{Z})^*$ contains an element \bar{u} of order 3. So $3 \mid p - 1$, $p \equiv 1 \pmod{3}$, but $p \equiv (-1)^{2^n} + 1 \equiv 2 \equiv -1 \pmod{3}$: this is a contradiction, so 3 is a primitive root modulo $p = 2^{2^n} + 1$. \square

Ex. 4.7 Suppose that p is a prime of the form $8t + 3$ and that $q = (p - 1)/2$ is also a prime. Show that 2 is a primitive root modulo p .

Proof. The first examples of such couples (q, p) are $(5, 11)$, $(29, 59)$, $(41, 83)$, $(53, 107)$, $(89, 179)$.
 $p = 2q + 1 = 8t + 3$ and p, q are prime numbers.

From Fermat's little theorem, $2^{p-1} \equiv 1 \pmod{p}$, so $2^{2q} \equiv 1 \pmod{p}$.

The order of 2 modulo p divides $2q$: to prove that the order of 2 is $2q = p - 1$, it is sufficient to prove

$$2^2 \not\equiv 1 \pmod{p}, \quad 2^q \not\equiv 1 \pmod{p}.$$

If $2^2 \equiv 1 \pmod{p}$, then $p \mid 3$, $p = 3$ and $q = 1$: q is not a prime, so $2^2 \not\equiv 1 \pmod{p}$.

If $2^q = 2^{(p-1)/2} \equiv 1 \pmod{p}$, then 2 is a square modulo p (prop. 4.2.1) : there exists $a \in \mathbb{Z}$ such that $2 \equiv a^2 \pmod{p}$.

From the complementary case of the law of quadratic reciprocity (see next chapter, prop. 5.1.3), 2 is a square modulo p iff

$$1 = \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Yet $p \equiv 3 \pmod{8}$, so $p^2 \equiv 9 \pmod{16}$, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = -1$, so 2 is not a square modulo p . This is a contradiction, so $2^q \not\equiv 1 \pmod{p}$: 2 is a primitive root modulo p . \square

Ex. 4.8 Let p be an odd prime. Show that a is a primitive root modulo p iff $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all prime divisors q of $p-1$.

Proof. • If a is a primitive root, then $a^k \not\equiv 1$ for all k , $1 \leq k < p-1$, so $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all prime divisors q of $p-1$.

• In the other direction, suppose $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all prime divisors q of $p-1$.

Let δ the order of a , and $p-1 = q_1^{a_1} q_2^{a_2} \cdots q_k^{a_k}$ the decomposition of $p-1$ in prime factors. As $\delta \mid p-1$, $\delta = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k}$, with $b_i \leq a_i$, $i = 1, 2, \dots, k$. If $b_i < a_i$ for some index i , then $\delta \mid (p-1)/q_i$, so $a^{(p-1)/q_i} \equiv 1 \pmod{p}$, which is in contradiction with the hypothesis. Thus $b_i = a_i$ for all i , and $\delta = q-1$: a is a primitive root modulo p . \square

Ex. 4.9 Show that the product of all the primitive roots modulo p is congruent to $(-1)^{\phi(p-1)}$ modulo p .

Proof. Here we suppose p prime, $p > 2$. Let g a primitive root modulo p . $U(\mathbb{Z}/p\mathbb{Z})$ is cyclic, generated by \bar{g} :

$$U(\mathbb{Z}/p\mathbb{Z}) = \{\bar{1}, \bar{g}, \bar{g}^2, \dots, \bar{g}^{p-2}\}, \quad \bar{g}^{p-1} = \bar{1}.$$

\bar{g}^k is a primitive element iff $k \wedge (p-1) = 1$, so the product of primitive elements in $U(\mathbb{Z}/p\mathbb{Z})$ is

$$\bar{P} = \prod_{\substack{k \wedge (p-1) = 1 \\ 1 \leq k < p-1}} \bar{g}^k.$$

so $\bar{P} = \bar{g}^S$, where $S = \sum_{\substack{k \wedge (p-1) = 1 \\ 1 \leq k < p-1}} k$.

From Ex. 2.22, we know that for $n \geq 2$,

$$\sum_{\substack{k \wedge n = 1 \\ 1 \leq k < n}} k = \frac{1}{2} n \phi(n).$$

So $S = \sum_{\substack{k \wedge (p-1) = 1 \\ 1 \leq k < p-1}} k = \frac{1}{2} (p-1) \phi(p-1)$.

As $p > 2$, $p-1$ is even. $(\bar{g}^{(p-1)/2})^2 = \bar{g}^{p-1} = \bar{1}$, and $\bar{g}^{(p-1)/2} \neq \bar{1}$. As $\mathbb{Z}/p\mathbb{Z}$ is a field, $\bar{g}^{(p-1)/2} = -\bar{1}$.

Thus $\bar{P} = (-\bar{1})^{\phi(p-1)}$: so the product P of all the primitive roots modulo p is such that

$$P \equiv (-1)^{\phi(p-1)} \pmod{p}.$$

\square

Ex. 4.10 Show that the sum of all the primitive roots modulo p is congruent to $\mu(p-1)$ modulo p .

Proof. Notation : $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the field with p elements, $|x|$ the multiplicative order of an element $x \in \mathbb{F}_p^*$, $\mathbb{N}^* = \{1, 2, 3, \dots\}$.

Let

$$\psi : \begin{cases} \mathbb{N}^* & \rightarrow \\ n & \mapsto \psi(n) = \sum_{d \in \mathbb{F}_p^*, |d|=n} d \end{cases}$$

$\psi(n)$ is the sum of the elements with order n in \mathbb{F}_p^* . So $\psi(n) = 0$ if $n \nmid p-1$, and $S = \psi(p-1)$ is the sought sum of all the primitive roots modulo p .

We compute for all $n \in \mathbb{N}^*$

$$f(n) = \sum_{d|n} \psi(d).$$

$f(n)$ is the sum of elements whose order divides n , in other words the sum of the roots of $x^n - 1$. This sum is, up to the sign, the coefficient of x^{n-1} , so is null, except in the case $n = 1$, where the sum of the unique root 1 of $x - 1$ is 1. So

$$f(1) = 1, \quad \forall n > 1, f(n) = 0,$$

($f = \chi_{\{1\}}$ is the characteristic function of $\{1\}$).

From the Möbius inversion formula, for all $n \in \mathbb{N}^*$, $\psi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$, so

$$\psi(p-1) = \sum_{d|p-1} \mu\left(\frac{p-1}{d}\right) f(d) = \mu(p-1).$$

Conclusion :

$$S = \sum_{d \in \mathbb{F}_p^*, |d|=p-1} d = \mu(p-1) :$$

the sum of all the primitive roots modulo p is congruent to $\mu(p-1)$ modulo p . \square

Ex. 4.11 Prove that $1^k + 2^k + \dots + (p-1)^k \equiv 0 \pmod{p}$ if $p-1 \nmid k$, and $-1 \pmod{p}$ if $p-1 \mid k$.

Proof. Let $S_k = 1^k + 2^k + \dots + (p-1)^k$.

Let g a primitive root modulo p : \bar{g} a generator of \mathbb{F}_p^* .

As $(\bar{1}, \bar{g}, \bar{g}^2, \dots, \bar{g}^{p-2})$ is a permutation of $(\bar{1}, \bar{2}, \dots, \overline{p-1})$,

$$\begin{aligned} \overline{S_k} &= \bar{1}^k + \bar{2}^k + \dots + \overline{p-1}^k \\ &= \sum_{i=0}^{p-2} \bar{g}^{ki} = \begin{cases} \overline{p-1} = -\bar{1} & \text{if } p-1 \mid k \\ \frac{\bar{g}^{(p-1)k} - 1}{\bar{g}^k - 1} = \bar{0} & \text{if } p-1 \nmid k \end{cases} \end{aligned}$$

since $p-1 \mid k \iff \bar{g}^k = \bar{1}$.

Conclusion :

$$\begin{aligned} 1^k + 2^k + \dots + (p-1)^k &\equiv 0 \pmod{p} \text{ if } p-1 \nmid k \\ 1^k + 2^k + \dots + (p-1)^k &\equiv -1 \pmod{p} \text{ if } p-1 \mid k \end{aligned}$$

\square

Ex. 4.12 Use the existence of a primitive root to give another proof of Wilson's theorem $(p-1)! \equiv -1 \pmod{p}$.

Proof. As the result is trivial if $p = 2$, we suppose that p is an odd prime.

Let g a primitive root modulo p : \bar{g} a generator of \mathbb{F}_p^* .

As $(\bar{g}^{(p-1)/2})^2 = \bar{g}^{p-1} = \bar{1}$, and $\bar{g}^{(p-1)/2} \neq 1$ in the field \mathbb{F}_p^* , then $\bar{g}^{(p-1)/2} = -1$, and $(\bar{1}, \bar{g}, \bar{g}^2, \dots, \bar{g}^{p-2})$ is a permutation of $(\bar{1}, \bar{2}, \dots, \overline{p-1})$, so

$$\begin{aligned} \overline{(p-1)!} &= \prod_{k=0}^{p-2} \bar{g}^k \\ &= \bar{g}^{\sum_{k=0}^{p-2} k} \\ &= \bar{g}^{(p-2)(p-1)/2} \\ &= \left(\bar{g}^{(p-1)/2}\right)^{p-2} \\ &= (-\bar{1})^{p-2} \\ &= -1. \end{aligned}$$

Hence $(p-1)! \equiv -1 \pmod{p}$ for each prime p . □

Ex. 4.13 Let G be a finite cyclic group and $g \in G$ a generator. Show that all the other generators are of the form g^k , where $(k, n) = 1$, n being the order of G .

Proof. Suppose $G = \langle g \rangle$, with $\text{Card } G = n$, so the order of g is n .

Let x another generator of G , then $x = g^k$, and $g = x^l$, $k, l \in \mathbb{Z}$, so $g = g^{kl}$, $g^{kl-1} = e$: $n \mid kl - 1$, then $kl - 1 = qn$, $q \in \mathbb{Z}$, so $n \wedge k = 1$.

Conversely, if $u \wedge k = 1$, there exist $u, v \in \mathbb{Z}$ such that $un + vk = 1$, so $g = g^{un+vk} = (g^n)^u (g^k)^v = x^v \in \langle x \rangle$, so $G \subset \langle x \rangle$, $G = \langle x \rangle$: x is a generator of G .

Conclusion : if g is a generator of G , all the other generators are the elements g^k , where $k \wedge n = 1$, $n = |G|$. □

Ex. 4.14 Let A be a finite abelian group and $a, b \in A$ elements of order m and n , respectively. If $(m, n) = 1$, prove that ab has order mn .

Proof. Suppose $|a| = m$, $|b| = n$, $m \wedge n = 1$.

• If $(ab)^k = e$, then $a^k = b^{-k}$, so $a^{kn} = b^{-kn} = (b^n)^{-k} = e$, so $m \mid kn$, with $m \wedge n = 1$, so $m \mid k$.

Similarly, $b^{km} = a^{-km} = (a^m)^{-k} = e$, so $n \mid km$, $n \wedge m = 1$: $n \mid k$.

As $n \mid k$, $m \mid k$, $n \wedge m = 1$, $nm \mid k$.

• Conversely, if $nm \mid k$, $k = qnm$, $q \in \mathbb{Z}$, so $(ab)^k = a^k b^k = (a^m)^{qn} (b^n)^{qm} = e$.

$$\forall k \in \mathbb{Z}, (ab)^k = e \iff nm \mid k.$$

So $|ab| = nm$. □

Ex. 4.15 Let K be a field and $G \subset K^*$ a finite subgroup of the multiplicative group of K . Extend the arguments used in the proof of Theorem 4.1 to show that G is cyclic.

Solution 1.

Proof. Let $n = |G|$. From Lagrange's theorem, $a^n = 1$ for all $a \in G$, so the polynomial $x^n - 1 \in K[x]$ has exactly n roots in G , and so

$$\forall x \in K, x \in G \iff x^n = 1.$$

If $d \mid n$, the polynomial $x^d - 1 \in K[x]$ has exactly d roots in K otherwise $x^n - 1 = (x^d - 1)g(x)$, $g(x) \in K[x]$, and $\deg(g) = n - d$ has at most $n - d$ roots, so $x^n - 1$ would have less than n roots in K . As $x_0^d = 1 \Rightarrow x_0^n = 1$, all these roots are in G : $x^d - 1$ has d roots in G .

Let $\psi(d)$ the number of elements in G of order d ($\psi(d) = 0$ if $d \nmid n$). Then $\sum_{c \mid d} \psi(c) = d$. Applying the Möbius inversion theorem, $\psi(d) = \sum_{c \mid d} \mu(c) d/c = \phi(d)$ (Prop. 2.2.5), in particular, $\psi(n) = \phi(n) \geq 1$. This proves the existence of an element of order n in G , so G is cyclic.

(variation : $\psi(d) = 0$ if there exists no element of order d , and $\psi(d) = \phi(d)$ otherwise : see Ex.4.13. So $\psi(d) \leq \phi(d)$ for all $d \mid n$. As $\sum_{d \mid n} \psi(d) = \sum_{d \mid n} \phi(d) = n$, $\psi(d) = \phi(d)$ for all $d \mid n$. So there exists in G an element of order n , and G is cyclic.) \square

Solution 2.

Proof. Let $n = |G| = p_1^{a_1} \cdots p_k^{a_k}$. From Lagrange's theorem, $y^n = 1$ for all $y \in G$.

$p(x) = x^{n/p_1} - 1 \in K[x]$ has at most $n/p_1 < n$ roots in K^* , a fortiori in G , so there exists $a \in G$ such that $a^{n/p_1} \neq 1$.

Let $c_1 = a^{n/p_1^{a_1}} = a^{p_2^{a_2} \cdots p_k^{a_k}}$. Then $c_1^{p_1^{a_1}} = 1$ and $c_1^{p_1^{a_1-1}} = a^{n/p_1} \neq 1$, so $|c_1| = p_1^{a_1}$.

Similarly, there exist c_2, \dots, c_k with respective orders $|c_i| = p_i^{a_i}$.

From exercise 4.14, we obtain by induction that $c = c_1 \cdots c_k$ has order $p_1^{a_1} \cdots p_k^{a_k} = n$, so G is cyclic. \square

Ex. 4.16 Calculate the solutions to $x^3 \equiv 1 \pmod{19}$ and $x^4 \equiv 1 \pmod{17}$.

Proof. Here we note a the class of x in $\mathbb{Z}/p\mathbb{Z}$.

Let $a \in \mathbb{F}_{19}$. Then

$$a^3 - 1 = 0 \iff a - 1 = 0 \text{ or } a^2 + a + 1 = 0.$$

$$\begin{aligned} a^2 + a + 1 = 0 &\iff (a + 10) - 99 = 0 \\ &\iff (a + 10)^2 - 4 = 0 \\ &\iff (a + 8)(a + 12) = 0 \end{aligned}$$

So, for all $x \in \mathbb{Z}$,

$$x^3 \equiv 1 \pmod{19} \iff x \equiv 1, 7, 11 \pmod{19}.$$

Let $a \in \mathbb{F}_{17}$.

$$\begin{aligned} a^4 = 1 &\iff a^2 = 1 \text{ or } a^2 = -1 = 4^2 \\ &\iff a = \pm 1 \text{ or } a = \pm 4 \end{aligned}$$

So, for all $x \in \mathbb{Z}$,

$$x^4 \equiv 1 \pmod{17} \iff x \equiv -1, 1, -4, 4 \pmod{17}.$$

Alternatively, we can take primitives roots modulo 19 and 17.
2 is a primitive root modulo 19, Let $a = 2^k \in \mathbb{F}_{19}$.

$$\begin{aligned} a^3 = 1 &\iff 2^{3k} = 1 \\ &\iff 18 \mid 3k \\ &\iff 6 \mid k \\ &\iff a = 1, 2^6 = 7, 2^{12} = 11 \end{aligned}$$

3 is a primitive root modulo 17. Let $a = 3^k \in \mathbb{F}_{17}$.

$$\begin{aligned} a^4 = 1 &\iff 3^{4k} = 1 \\ &\iff 16 \mid 4k \\ &\iff 4 \mid k \\ &\iff a = 1, 3^4 = -4, 3^8 = -1, 3^{12} = 4 \end{aligned}$$

□

Ex. 4.17 Use the fact that 2 is a primitive root modulo 29 to find the seven solutions to $x^7 \equiv 1 \pmod{29}$.

Proof. Let $x \in \mathbb{Z}$, then $x \equiv 2^k \pmod{29}, k \in \mathbb{N}$.

$$\begin{aligned} x^7 \equiv 1 \pmod{29} &\iff 2^{7k} \equiv 1 \pmod{29} \\ &\iff 28 \mid 7k \\ &\iff 4 \mid k \end{aligned}$$

So the group cyclic S of the roots of $x^7 - 1$ in \mathbb{F}_{29} are

$$\begin{aligned} S &= \{1, 2^4, 2^8, 2^{12}, 2^{16}, 2^{20}, 2^{24}\}, \\ S &= \{1, 16, 24, 7, 25, 23, 20\}. \end{aligned}$$

□

Ex. 4.18 Solve the congruence $1 + x + \cdots + x^6 \equiv 0 \pmod{29}$.

Proof. As $(1 + x + \cdots + x^6)(1 - x) = 1 - x^7$,

$$1 + x + \cdots + x^6 \equiv 0 \pmod{29} \iff \begin{cases} x^7 \equiv 1 \pmod{29} \\ x \not\equiv 1 \pmod{29} \end{cases}$$

From Ex. 4.17, the solutions are congruent to $2^4, 2^8, 2^{12}, 2^{16}, 2^{20}, 2^{24}$ modulo 29. □

Ex. 4.19 Determine the numbers a such that $x^3 \equiv a \pmod{p}$ is solvable for $p = 7, 11, 13$.

Proof. (a) If $p = 7$, then $3 \mid p - 1, d = 3 \wedge (p - 1) = 3$. From Prop. 4.2.1,

$$\exists x \in \mathbb{Z}, a \equiv x^3 \pmod{7} \iff a \equiv 0 \pmod{7} \text{ or } a^{(p-1)/3} = a^2 \equiv 1 \pmod{7}.$$

So the numbers a such that $x^3 \equiv a \pmod{7}$ is solvable are congruent at $0, 1, -1$ modulo 7.

(b) If $p = 11$, then $d = 3 \wedge (p - 1) = 1$. With the same proposition,

$$\exists x \in \mathbb{Z}, a \equiv x^3 \pmod{11} \iff a \equiv 0 \pmod{11} \text{ or } a^{p-1} = a^6 \equiv 1 \pmod{11}.$$

So all integers a are cube modulo 11, in only one way.

For an alternative proof, the application

$$f : \begin{cases} \mathbb{F}_{11}^* & \rightarrow \mathbb{F}_{11}^* \\ x & \mapsto x^3 \end{cases}$$

f is a bijection. Indeed,

- f is a group homomorphism,
- $x^3 = 1 \Rightarrow (x^3)^7 = 1 \Rightarrow x = 1$ so $\ker(f) = \{1\}$,
- $f : \mathbb{F}_{11}^* \rightarrow \mathbb{F}_{11}^*$ is injective and \mathbb{F}_{11}^* is finite, so f is bijective.

In \mathbb{F}_{11} , $0 = 0^3, 1 = 1^3, 2 = 7^3, 3 = 9^3, 4 = 5^3, 5 = 3^3, 6 = 8^3, 7 = 6^3, 8 = 2^3, 9 = 4^3, 10 = 10^3$.

(c) If $p = 13$, then $3 \mid p - 1, 3 \wedge (p - 1) = 3$, so

$$\begin{aligned} \exists x \in \mathbb{Z}, a \equiv x^3 \pmod{13} &\iff a \equiv 0 \pmod{13} \text{ or } a^{(p-1)/3} = a^4 \equiv 1 \pmod{13} \\ &\iff a \equiv 0, 1, -1, 5, -5 \pmod{13} \end{aligned}$$

$$(5 \equiv 8^3 \pmod{13}).$$

□

Ex. 4.20 Let p be a prime, and d a divisor of $p - 1$. Show that d th powers form a subgroup of $U(\mathbb{Z}/p\mathbb{Z})$ of order $(p - 1)/d$. Calculate this subgroup for $p = 11, d = 5$, for $p = 17, d = 4$, and for $p = 19, d = 6$.

Proof. Here p is a prime number, and $d \mid p - 1$. Let

$$f : \begin{cases} \mathbb{F}_p^* & \rightarrow \mathbb{F}_p^* \\ x & \rightarrow x^d \end{cases}$$

Then f is a group homomorphism, and $\text{im}(f)$ is the set of d th powers, and consequently is a subgroup of $U(\mathbb{F}_p) = \mathbb{F}_p^*$. $\ker(f)$ is the group of the roots of $x^d - 1$. As $d \mid p - 1$, the polynomial $x^d - 1$ has exactly d roots (Prop. 4.1.2), so $|\ker(f)| = d$.

As $\text{im}(f) \simeq \mathbb{F}_p^* / \ker(f)$,

$$|\text{im}(f)| = |\mathbb{F}_p^*| / |\ker(f)| = (p - 1)/d.$$

So there exist exactly $(p - 1)/d$ d th powers in $(\mathbb{Z}/p\mathbb{Z})^*$.

From Prop. 4.2.1, as $d \mid p - 1, d \wedge (p - 1) = d$, for all $x \in \mathbb{F}_p^*$,

$$x \in \text{im}(f) \iff x^{(p-1)/d} = 1.$$

So the group of d th powers is the group of the roots of $x^{(p-1)/d} - 1$.

- If $p = 11, d = 5$, $\text{im}(f) = \{1, -1\}$.
- If $p = 17, d = 4$, $x \in \text{im}(f) \iff x^4 = 1 : \text{im}(f) = \{1, -1, 4, -4\}$.
- If $p = 19, d = 6$, $x \in \text{im}(f) \iff x^3 = 1 : \text{im}(f) = \{1, 7, 7^2 = 11\}$, where $7 \equiv 2^6 \pmod{19}$.

□

Ex. 4.21 If g is a primitive root modulo p , and $d \mid p-1$, show that $g^{(p-1)/d}$ has order d . Show also that a is a d th power iff $a \equiv g^{kd} \pmod{p}$ for some k . Do Exercises 16-20 making use of those observations.

Proof. Let $x = \bar{g}^{(p-1)/d} \in \mathbb{F}_p^*$, where g is a primitive root modulo p . For all $k \in \mathbb{Z}$,

$$\begin{aligned} x^k = 1 &\iff g^{k \frac{p-1}{d}} = 1 \\ &\iff p-1 \mid k \frac{p-1}{d} \\ &\iff d \mid k \end{aligned}$$

So the order of $\bar{g}^{(p-1)/d}$ is d .

- If $\bar{a} = \bar{g}^{kd}$, then $\bar{a} = x^k$, where $x = \bar{g}^{(p-1)/d}$, so \bar{a} is a d th power.
- If $\bar{a} \neq \bar{0}$ is a d th power, $\bar{a} = x^k, x \in \mathbb{F}_p^*$. As $x \in \langle \bar{g} \rangle$, $x = \bar{g}^k$, so $\bar{a} = \bar{g}^{kd}$.

So, if $a \not\equiv 0 \pmod{p}$, a is a d th power iff $a \equiv g^{kd} \pmod{p}$ for some k .

By example (Ex. 4.20), 2 is a primitive root modulo 19, so the 6th powers modulo 19 are $2^0 = 1, 2^6 = 7, 2^{12} = 11$. \square

Ex. 4.22 If a has order 3 modulo p , show that $1+a$ has order 6.

Proof. If a has order 3 modulo p , then $0 \equiv a^3 - 1 = (a-1)(a^2 + a + 1) \pmod{p}$, with $a \not\equiv 1 \pmod{p}$, so $a^2 + a + 1 \equiv 0 \pmod{p}$. Thus

$$\begin{aligned} (1+a)^3 &\equiv 1 + 3a + 3a^2 + a^3 \\ &\equiv 1 + 3a + 3(-1-a) + 1 \\ &\equiv -1 \pmod{p} \end{aligned}$$

So $(1+a)^6 \equiv 1 \pmod{p}$.

$$(1+a)^2 \equiv 1 + 2a + a^2 = 1 + 2a + (-1-a) \equiv a \not\equiv 1 \pmod{p}.$$

So $(1+a)^6 \equiv 1, (1+a)^2 \not\equiv 1, (1+a)^3 \not\equiv 1 \pmod{p}$, so the order of $1+a$ divides 6, but doesn't divide 2 or 3, so $1+a$ has order 6 modulo p . \square

Ex. 4.23 Show that $x^2 \equiv -1 \pmod{p}$ has a solution iff $p \equiv 1 \pmod{4}$, and that $x^4 \equiv -1 \pmod{p}$ has a solution iff $p \equiv 1 \pmod{8}$.

Proof. If $x^2 \equiv -1 \pmod{p}$, then \bar{x} has order 4 in \mathbb{F}_p^* , hence from Lagrange's theorem, $4 \mid p-1$.

Conversely, suppose $4 \mid p-1$, so $p = 4k+1, k \in \mathbb{N}^*$. From proposition 4.2.1, as $2 \mid p-1$, -1 is a square modulo p iff $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$, which is true because $(-1)^{(p-1)/2} = (-1)^{2k} = 1$.

If $x^4 \equiv -1 \pmod{p}$, then $\bar{x}^8 = 1 \in \mathbb{F}_p^*$, and $\bar{x}^4 \neq 1$, so \bar{x} has order 8 in \mathbb{F}_p^* , so $8 \mid p-1$.

Conversely, if $p \equiv 1 \pmod{8}$, $p = 8K+1, K \in \mathbb{N}^*$. From Prop.4.2.1, as $4 \mid p-1$, there exists $x \in \mathbb{Z}$ such that $-1 = x^4$ iff $(-1)^{(p-1)/4} \equiv 1 \pmod{8}$, which is true because $(-1)^{(p-1)/4} = (-1)^{2K} = 1$.

Conclusion :

$$\exists x \in \mathbb{Z}, x^4 \equiv -1 \pmod{p} \iff p \equiv 1 \pmod{8}.$$

\square

Ex. 4.24 Show that $ax^m + by^n \equiv c \pmod{p}$ has the same number of solutions as $ax^{m'} + by^{n'} \equiv c \pmod{p}$, where $m' = (m, p-1)$ and $n' = (n, p-1)$.

Proof. If $a \wedge b \nmid c$, the two equations have no solution. So we can suppose $a \wedge b \mid c$, and after division by $\delta = a \wedge b$, we obtain an equation $a'x^m + b'y^n = c'$, $a' = a/\delta, b' = b\delta, c' = c\delta$, and $a' \wedge b' = 1$. So it remains to prove that $ax^m + by^n \equiv c \pmod{p}$ has the same number of solutions as $ax^{m'} + by^{n'} \equiv c \pmod{p}$ when $a \wedge b = 1$.

In this case the equation $au + bv = c$ has solutions. Let N the number of solutions (\bar{x}, \bar{y}) of the equation $\bar{a}\bar{x}^m + \bar{b}\bar{y}^n = \bar{c}$, N' the number of solutions (\bar{x}, \bar{y}) of the equation $\bar{a}\bar{x}^{m'} + \bar{b}\bar{y}^{n'} = \bar{c}$. Then

$$\begin{aligned} N &= \text{Card}\{(\bar{x}, \bar{y}) \in \mathbb{F}_p \times \mathbb{F}_p \mid \bar{a}\bar{x}^m + \bar{b}\bar{y}^n = \bar{c}\} \\ &= \sum_{\bar{a}\bar{u} + \bar{b}\bar{v} = \bar{c}} \text{Card}\{(\bar{x}, \bar{y}) \in \mathbb{F}_p \times \mathbb{F}_p \mid \bar{x}^m = \bar{u}, \bar{y}^n = \bar{v}\} \\ &= \sum_{\bar{a}\bar{u} + \bar{b}\bar{v} = \bar{c}} \text{Card}\{\bar{x} \in \mathbb{F}_p \mid \bar{x}^m = \bar{u}\} \times \text{Card}\{\bar{y} \in \mathbb{F}_p \mid \bar{y}^n = \bar{v}\}. \end{aligned}$$

The same is true for N' , so it is sufficient to prove that

$$\text{Card}\{\bar{x} \in \mathbb{F}_p \mid \bar{x}^m = \bar{u}\} = \text{Card}\{\bar{x} \in \mathbb{F}_p \mid \bar{x}^{m'} = \bar{u}\},$$

where $m' = m \wedge (p-1)$, and a similar equality for the equation $\bar{y}^n = \bar{v}$.

Let \bar{g} a generator of \mathbb{F}_p^* . Write $\bar{u} = \bar{g}^r, r \in \mathbb{N}$.

$$\begin{aligned} \exists \bar{x} \in \mathbb{F}_p, \bar{x}^m = \bar{u} &\iff \exists k \in \mathbb{Z}, \bar{g}^{mk} = \bar{g}^r \\ &\iff \exists k \in \mathbb{Z}, p-1 \mid mk - r \\ &\iff \exists k \in \mathbb{Z}, \exists l \in \mathbb{Z}, r = mk + l(p-1) \\ &\iff m \wedge (p-1) \mid r \end{aligned}$$

So

$$\{\bar{x} \in \mathbb{F}_p \mid \bar{x}^m = \bar{u}\} \neq \emptyset \iff m \wedge (p-1) \mid r,$$

and similarly

$$\{\bar{x} \in \mathbb{F}_p \mid \bar{x}^{m'} = \bar{u}\} \neq \emptyset \iff m' \wedge (p-1) \mid r.$$

Since $m' \wedge (p-1) = (m \wedge (p-1)) \wedge (p-1) = m \wedge (p-1)$, these two conditions are equivalent, so these two sets are empty for the same values of \bar{u} .

Let \bar{u} is such that $\{\bar{x} \in \mathbb{F}_p \mid \bar{x}^m = \bar{u}\} \neq \emptyset$, and x_0 a fixed solution of $\bar{x}^m = \bar{u}$.

Write $\bar{x} = \bar{g}^k, \bar{x}_0 = \bar{g}^{k_0}$. Let $d = m \wedge (p-1) (= m')$.

$$\begin{aligned} \bar{x}^m = u &\iff \bar{x}^m = \bar{x}_0^m \\ &\iff \bar{g}^{mk} = \bar{g}^{mk_0} \\ &\iff p-1 \mid m(k - k_0) \\ &\iff \frac{p-1}{d} \mid \frac{m}{d}(k - k_0) \\ &\iff \frac{p-1}{d} \mid k - k_0 \\ &\iff \exists j \in \mathbb{Z}, k = k_0 + j \frac{p-1}{d} \end{aligned}$$

As g is a primitive root modulo p , the distinct solutions are $x_0, x_0 g^{\frac{p-1}{d}}, \dots, x_0 g^{k \frac{p-1}{d}}, \dots, x_0 g^{(d-1) \frac{p-1}{d}}$, so in this case

$$\text{Card}\{\bar{x} \in \mathbb{F}_p \mid \bar{x}^m = \bar{u}\} = d = m \wedge (p-1).$$

As $m' \wedge (p-1) = m \wedge (p-1)$,

$$\text{Card}\{\bar{x} \in \mathbb{F}_p \mid \bar{x}^m = \bar{u}\} = \text{Card}\{\bar{x} \in \mathbb{F}_p \mid \bar{x}^{m'} = \bar{u}\}.$$

So $N = N' : ax^m + by^n \equiv c \pmod{p}$ has the same number of solutions as $ax^{m'} + by^{n'} \equiv c \pmod{p}$, where $m' = (m, p-1)$ and $n' = (n, p-1)$. \square

Ex. 4.25 Prove Propositions 4.2.2 and 4.2.4.

Proposition 4.2.2. Suppose that a is odd, $e \geq 3$, and consider the congruence $x^n \equiv a \pmod{2^e}$. If n is odd, a solution always exists and it is unique.

If n is even, a solution exists iff $a \equiv 1 \pmod{4}$, $a^{2^{e-2}/d} \equiv 1 \pmod{2^e}$, where $d = (n, 2^{e-2})$. When a solution exists there are exactly $2d$ solutions.

Proof. We suppose that a is odd and $e \geq 3$.

From Theorem 2', we know that $\{(-1)^a 5^b \mid 0 \leq a \leq 1, 0 \leq b \leq 2^{e-2}\}$ constitutes a reduced residue system modulo 2^e , so we can write

$$\begin{aligned} a &\equiv (-1)^s 5^t \pmod{2^e}, 0 \leq s \leq 1, 0 \leq t \leq 2^{e-2}, \\ x &\equiv (-1)^y 5^z \pmod{2^e}, 0 \leq y \leq 1, 0 \leq z \leq 2^{e-2}. \end{aligned}$$

For all $x \in \mathbb{Z}$,

$$x^n \equiv a \pmod{2^e} \iff (-1)^{ny} 5^{nz} \equiv (-1)^s 5^t \pmod{2^e}$$

Then $(-1)^{ny} \equiv (-1)^s \pmod{4}$, $ny \equiv s \pmod{2}$, $(-1)^{ny} = (-1)^s$, so $5^{nz} \equiv 5^t \pmod{2^e}$.

Conversely, if $ny \equiv s \pmod{2}$ and $5^{nz} \equiv 5^t \pmod{2^e}$, then $x^n \equiv a \pmod{2^e}$, so

$$x^n \equiv a \pmod{2^e} \iff \begin{cases} ny \equiv s \pmod{2} \\ 5^{nz} \equiv 5^t \pmod{2^e} \end{cases} \iff \begin{cases} ny \equiv s \pmod{2} \\ nz \equiv t \pmod{2^{e-2}} \end{cases}$$

since the order of 5 modulo 2^e is 2^{e-2} .

• Suppose that n is an odd integer. Then

$$\begin{cases} ny \equiv s \pmod{2} \\ nz \equiv t \pmod{2^{e-2}} \end{cases} \iff \begin{cases} y \equiv s \pmod{2} \\ z \equiv n't \pmod{2^{e-2}} \end{cases}$$

where n' is an inverse of n modulo 2^{e-2} : $nn' \equiv 1 \pmod{2^{e-2}}$.

So $x^n \equiv a \pmod{2^e}$ has an unique solution modulo 2^e .

• Suppose that n is an even integer.

Then $\begin{cases} ny \equiv s \pmod{2} \\ nz \equiv t \pmod{2^{e-2}} \end{cases}$ implies $s \equiv 0 \pmod{2}$ and $d = n \wedge 2^{e-2} \mid t$.

Then $a \equiv (-1)^s 5^t \equiv 5^t \pmod{2^e}$, so $a \equiv 1 \pmod{4}$.

Hence $a^{\frac{2^{e-2}}{d}} \equiv \left(5^{2^{e-2}}\right)^{\frac{t}{d}} \equiv 1 \pmod{2^e}$, since 5 has order 2^{e-2} , and $d \mid t$.

So, if n is even, and $d = n \wedge 2^{e-2}$,

$$\exists x \in \mathbb{Z}, x^n \equiv a \pmod{2^e} \Rightarrow \begin{cases} a \equiv 1 \pmod{4}, \\ a^{\frac{2^{e-2}}{d}} \equiv 1 \pmod{2^e}. \end{cases}$$

Conversely, suppose that $\begin{cases} a & \equiv 1 \pmod{4}, \\ a^{\frac{2^{e-2}}{d}} & \equiv 1 \pmod{2^e}. \end{cases}$

Then $a \equiv (-1)^s 5^t \pmod{2^e}$ implies $a \equiv (-1)^s \pmod{4}$, so s is even, and $a \equiv 5^t \pmod{2^e}$.

Therefore $5^{t\frac{2^{e-2}}{d}} \equiv 1 \pmod{2^e}$, which implies $2^{e-2} \mid t\frac{2^{e-2}}{d}$, so $d \mid t$.

$$\begin{aligned} \exists x \in \mathbb{Z}, x^n \equiv a \pmod{2^e} &\iff \exists y \in \mathbb{Z}, \exists z \in \mathbb{Z}, \begin{cases} ny & \equiv s \pmod{2} \\ nz & \equiv t \pmod{2^{e-2}} \end{cases} \\ &\iff \exists z \in \mathbb{Z}, nz \equiv t \pmod{2^{e-2}} \quad (\text{since } n, s \text{ even}) \\ &\iff \exists z \in \mathbb{Z}, 2^{e-2} \mid nz - t \\ &\iff \exists z \in \mathbb{Z}, \frac{2^{e-2}}{d} \mid \frac{n}{d}z - \frac{t}{d} \\ &\iff \exists z \in \mathbb{Z}, \exists q \in \mathbb{Z}, q\frac{2^{e-2}}{d} + z\frac{n}{d} = \frac{t}{d} \end{aligned}$$

As $\frac{2^{e-2}}{d} \wedge \frac{n}{d} = 1$, there exists a solution (q, z_0) of this last equation, where $0 \leq z_0 < \frac{2^{e-2}}{d}$, and so $x_0 = 5^{z_0}$ is a particular solution of $x^n \equiv a \pmod{2^e}$, therefore

$$\exists x \in \mathbb{Z}, x^n \equiv a \pmod{2^e} \iff \begin{cases} a & \equiv 1 \pmod{4} \\ a^{\frac{2^{e-2}}{d}} & \equiv 1 \pmod{2^e} \end{cases}$$

If there exists a particular solution $x_0 \equiv (-1)^{y_0} 5^{z_0}$, then

$$\begin{aligned} x^n \equiv a \pmod{2^e} &\iff x^n \equiv x_0^n \pmod{2^e} \\ &\iff \begin{cases} ny & \equiv ny_0 \pmod{2} \\ nz & \equiv nz_0 \pmod{2^{e-2}} \end{cases} \\ &\iff n(z - z_0) \equiv 0 \pmod{2^{e-2}} \quad (\text{since } n \text{ even}) \\ &\iff \frac{2^{e-2}}{d} \mid \frac{n}{d}(z - z_0) \\ &\iff \frac{2^{e-2}}{d} \mid z - z_0, \quad (\text{since } \frac{2^{e-2}}{d} \wedge \frac{n}{d} = 1) \\ &\iff \exists k \in \mathbb{Z}, z = z_0 + k\frac{2^{e-2}}{d} \end{aligned}$$

As the order of 5 modulo 2^e is 2^{e-2} , the solutions of $x^n \equiv a \pmod{2^e}$ are

$$x_k = (-1)^{y_0} 5^{z_0 + k\frac{2^{e-2}}{d}}, \quad 0 \leq y_0 < 2, \quad 0 \leq k < d,$$

so there are exactly $2d$ solutions modulo 2^e . □

Proposition 4.2.4. *Let 2^l be the highest power of 2 dividing n . Suppose that a is odd and that $x^n \equiv a \pmod{2^{2l+1}}$ is solvable. Then $x^n \equiv a \pmod{2^e}$ is solvable for all $e \geq 2l+1$ (and consequently for all $e \geq 1$). Moreover, all these congruences have the same number of solutions.*

Proof. We suppose that a is odd, and that $x^n \equiv a \pmod{2^{2l+1}}$ is solvable. l is such that $n = 2^l n'$, where n' is an odd integer.

Let the induction hypothesis be, for a fixed integer $m \geq 2l + 1$,

$$\exists x_0 \in \mathbb{Z}, x_0^n \equiv a \pmod{2^m}.$$

Let $x_1 = x_0 + b2^{m-l}$: we show that for an appropriate choice of $b \in \{0, 1\}$, $x_1^n \equiv a \pmod{2^{m+1}}$.

$$x_1^n = x_0^n + nb2^{m-l}x_0^{n-1} + 2^{2m-2l}A, \quad A \in \mathbb{Z}.$$

Since $m \geq 2l + 1$, $2m - 2l \geq m + 1$, so

$$x_1^n \equiv x_0^n + nb2^{m-l}x_0^{n-1} \pmod{2^{m+1}}.$$

$$\begin{aligned} x_1^n \equiv a \pmod{2^{m+1}} &\iff (x_0^n - a) + n'bx_0^{n-1}2^m \equiv 0 \pmod{2^{m+1}} \\ &\iff \frac{x_0^n - a}{2^m} + n'bx_0^{n-1} \equiv 0 \pmod{2} \end{aligned}$$

As a is odd, and $x_0^n \equiv a \pmod{2^m}$, $m \geq 1$, x_0 is odd, and n' is odd, so there exists a unique $b \in \{0, 1\}$ such that $\frac{x_0^n - a}{2^m} + n'bx_0^{n-1} \equiv 0 \pmod{2}$. So there exists $x_1 \in \mathbb{Z}$ such that $x_1^n \equiv a \pmod{2^{m+1}}$, and the induction is completed. Therefore, $x^n \equiv a \pmod{2^e}$ is solvable for all $e \geq 2l + 1$, and consequently for all $e \geq 1$.

From the Proposition 4.2.2., with the hypothesis $e \geq 3$, we know that the number of solutions of the solvable equation $x^n \equiv a \pmod{2^e}$, $e \geq 2l + 1$, is 1 if n is odd, $2(n \wedge 2^{e-2})$ if n is even.

If n is even, $l \geq 1$, $e \geq 2l + 1 \geq 3$. Since $e \geq 2l + 1$, and $n = 2^l n'$ for an odd n' , $l \leq \frac{e-1}{2} \leq e - 2$, so $n \wedge 2^{e-2} = n'2^l \wedge 2^{e-2} = 2^l$, and the number of solutions is 2^{l+1} , independent of $e \geq 2l + 1$.

Conclusion : under the hypothesis $x^n \equiv a \pmod{2^{2l+1}}$, where $l = \text{ord}_2(n)$, then $x^n \equiv a \pmod{2^e}$ is solvable for all $e \geq 1$, and all these congruences have the same number of solutions for $e \geq 2l + 1$, $e \geq 3$. \square

Chapter 5

Ex. 5.1 Use Gauss' lemma to determine $\left(\frac{5}{7}\right)$, $\left(\frac{3}{11}\right)$, $\left(\frac{6}{13}\right)$, $\left(\frac{-1}{p}\right)$.

Proof. • $a = 5, p = 7$.

The array of values of the least residues modulo $p = 7$, for $1 \leq k \leq (p-1)/2$.

$k \pmod{7}$	1	2	3
$5k \pmod{7}$	-2	3	1

So the number of negative least residues is $\mu = 1$, and $\left(\frac{5}{7}\right) = (-1)^\mu = -1$.

• $a = 3, p = 11$.

$k \pmod{11}$	1	2	3	4	5
$3k \pmod{11}$	3	-5	-2	1	4

So $\mu = 2$, $\left(\frac{3}{11}\right) = (-1)^\mu = 1$.

• $a = 6, p = 13$.

$k \pmod{13}$	1	2	3	4	5	6
$6k \pmod{13}$	6	-1	5	-2	4	-3

So $\mu = 3$, $\left(\frac{6}{13}\right) = (-1)^\mu = -1$.

• If $a = -1$, and p is an odd prime, the values of the least residues of $-k$ modulo p for $k = 1, 2, \dots, (p-1)/2$ are $-k$, all negative. So the number of negative least residues is $\mu = (p-1)/2$, and $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. \square

Ex. 5.2 Show that the number of solutions to $x^2 \equiv a \pmod{p}$ is equal to $1 + (a/p)$.

Proof. Let N the number of solutions of $x^2 \equiv a \pmod{p}$.

- If $(\frac{a}{p}) = 0$, then $p \mid a$, $a \equiv 0 \pmod{p}$, so the unique solution of $x^2 \equiv a = 0$ is $x \equiv 0 \pmod{p}$, so $N = 1 = 1 + (\frac{a}{p})$.
- If $(\frac{a}{p}) = -1$, then $N = 0 = 1 + (\frac{a}{p})$.
- If $(\frac{a}{p}) = 1$, then $x^2 \equiv a \pmod{p}$ has a solution x_0 , and $x^2 \equiv a \pmod{p} \iff x^2 \equiv x_0^2 \pmod{p} \iff p \mid (x - x_0)(x + x_0) \iff x \equiv \pm x_0 \pmod{p}$, so $N = 2 = 1 + (\frac{a}{p})$. \square

Ex. 5.3 Suppose $p \nmid a$. Show that the number of solutions to $ax^2 + bx + c \equiv 0 \pmod{p}$ is equal to $1 + ((b^2 - 4ac)/p)$.

Proof. Here p is an odd prime number, and $p \nmid a$. Let N be the number of solutions of $ax^2 + bx + c \equiv 0 \pmod{p}$

For $\bar{x} \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$,

$$\begin{aligned} \overline{a}\bar{x}^2 + \overline{b}\bar{x} + \overline{c} &= \overline{a} \left(\bar{x}^2 + \frac{\overline{b}}{\overline{a}} \bar{x} + \frac{\overline{c}}{\overline{a}} \right) \\ &= \overline{a} \left(\left(\bar{x} + \frac{\overline{b}}{2\overline{a}} \right)^2 - \frac{\overline{b}^2 - 4\overline{a}\overline{c}}{4\overline{a}^2} \right) \end{aligned}$$

Let $\Delta = b^2 - 4ac$. Then N is the number of solutions of $\left(\bar{x} + \frac{\overline{b}}{2\overline{a}} \right)^2 - \frac{\overline{\Delta}}{4\overline{a}^2} = \overline{0}$ in \mathbb{F}_p . As in Ex.5.2, $N = 1$ if $\overline{\Delta} = \overline{0}$, $N = 0$ if $\overline{\Delta}$ is not a square in \mathbb{F}_p^* , otherwise $\overline{\Delta} = \delta^2$, $\delta \in \mathbb{F}_p^*$, and the solutions are $\bar{x} = (-\overline{b} \pm \delta)/2\overline{a}$, so $N = 2$. In the three cases, $N = 1 + (\frac{\Delta}{p})$. \square

Ex. 5.4 Prove that $\sum_{a=1}^{p-1} (a/p) = 0$.

Proof. Here p is an odd prime (the result is false if $p = 2$). In the interval $[1, p-1]$, there exist $(p-1)/2$ residues, and $(p-1)/2$ nonresidues (Prop. 5.1.2., Corollary 1), so $\sum_{a=1}^{p-1} (a/p) = 0$. \square

Proof. As an alternative proof, let $S = \sum_{a=1}^{p-1} (\frac{a}{p})$, and b a nonresidue modulo p : $(\frac{b}{p}) = -1$ (such a b exists if $p \neq 2$). As $a \mapsto ab$ is a bijection from \mathbb{F}_p^* to itself,

$$\left(\frac{b}{p} \right) S = \sum_{a=1}^{p-1} \left(\frac{ab}{p} \right) = \sum_{c=1}^{p-1} \left(\frac{c}{p} \right) = S,$$

so $-S = S$, $S = 0$. \square

Ex. 5.5 Prove that $\sum_{x=1}^{p-1} ((ax+b)/p) = 0$ provided that $p \nmid a$.

There is a mistake in the sentence : we must read

Prove that $\sum_{x=0}^{p-1} ((ax+b)/p) = 0$ provided that $p \nmid a$.

For instance,

$$\sum_{x=1}^{5-1} \left(\frac{x+1}{5} \right) = \left(\frac{2}{5} \right) + \left(\frac{3}{5} \right) + \left(\frac{4}{5} \right) = -1 \neq 0.$$

Proof. From exercise 5.3, as $\left(\frac{0}{p}\right) = 0$, we know that

$$\sum_{\bar{x} \in \mathbb{F}_p} \left(\frac{x}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) = 0.$$

(This sum is well defined, since $\left(\frac{x}{p}\right)$ depends only of $\bar{x} : x \equiv x' \pmod{p} \Rightarrow \left(\frac{x}{p}\right) = \left(\frac{x'}{p}\right)$.)

As $\bar{a} \neq \bar{0}$ in \mathbb{F}_p , $f : \begin{cases} \mathbb{F}_p & \rightarrow \mathbb{F}_p \\ x & \mapsto \bar{a}x + \bar{b} \end{cases}$ is a bijection. Thus

$$\begin{aligned} \sum_{x=0}^{p-1} \left(\frac{ax+b}{p}\right) &= \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p}\right) \\ &= \sum_{y \in \mathbb{F}_p} \left(\frac{y}{p}\right) \quad (y = f(x)) \\ &= 0 \end{aligned}$$

□

Ex. 5.6 Show that the number of solutions to $x^2 - y^2 \equiv a \pmod{p}$ is given by:

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2 + a}{p}\right)\right).$$

Proof. Let $S = \{(\bar{x}, \bar{y}) \in \mathbb{F}_p^2 \mid \bar{x}^2 - \bar{y}^2 = \bar{a}\}$. From Ex.5.2,

$$\begin{aligned} |S| &= \sum_{\bar{y} \in \mathbb{F}_p} \text{Card} \{\bar{x} \in \mathbb{F}_p \mid \bar{x}^2 = \bar{y}^2 + \bar{a}\} \\ &= \sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2 + a}{p}\right)\right). \end{aligned}$$

□

Ex. 5.7 By calculating directly show that the number of solutions to $x^2 - y^2 \equiv a \pmod{p}$ is $p - 1$ if $p \nmid a$, and $2p - 1$ if $p \mid a$. (Hint. Use the change of variables $u = x + y, v = x - y$.)

Proof. Let $S = \{(\bar{x}, \bar{y}) \in \mathbb{F}_p^2 \mid \bar{x}^2 - \bar{y}^2 = \bar{a}\}$, and $T = \{(\bar{u}, \bar{v}) \in \mathbb{F}_p^2 \mid \bar{u}\bar{v} = \bar{a}\}$. Then $f : \begin{cases} S & \rightarrow T \\ (\bar{x}, \bar{y}) & \mapsto (\bar{x} + \bar{y}, \bar{x} - \bar{y}) \end{cases}$ is well defined (if $(\bar{x}, \bar{y}) \in S$, $(\bar{x} - \bar{y})(\bar{x} + \bar{y}) = a$, so $(\bar{x} + \bar{y}, \bar{x} - \bar{y}) \in T$). Moreover f is a bijection, with inverse $(\bar{u}, \bar{v}) \mapsto ((\bar{u} + \bar{v})/2, (\bar{u} - \bar{v})/2)$, so $|S| = |T|$.

We compute $|T|$.

- Suppose that $p \nmid a$, so $\bar{a} \neq \bar{0}$. For $\bar{v} = 0$, there is no solution, and for each $\bar{v} \neq 0$, we obtain the unique solution $(\bar{a}\bar{v}^{-1}, \bar{v})$, so there exist $p - 1$ solutions.

- Suppose that $p \mid a$. The solutions of $\bar{u}\bar{v} = \bar{0}$ are $(\bar{0}, \bar{0})$, $(\bar{0}, \bar{v})$ for each $\bar{v} \neq \bar{0}$, $(\bar{u}, \bar{0})$ for each $\bar{v} = \bar{0}$, that is to say $N = 1 + (p - 1) + (p - 1) = 2p - 1$ solutions.

Conclusion :

$$\begin{aligned} \text{Card } \{(\bar{x}, \bar{y}) \in \mathbb{F}_p^2 \mid \bar{x}^2 - \bar{y}^2 = \bar{a}\} &= p - 1 \quad \text{if } p \nmid a \\ &= 2p - 1 \quad \text{if } p \mid a \end{aligned}$$

□

Ex. 5.8 Combining the results of Ex. 5.6 and 5.7 show that:

$$\sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p} \right) = \begin{cases} -1 & \text{if } p \nmid a \\ p - 1 & \text{if } p \mid a \end{cases}$$

Proof. Let $S = \{(\bar{x}, \bar{y}) \in \mathbb{F}_p^2 \mid \bar{x}^2 - \bar{y}^2 = \bar{a}\}$.

We obtain in Ex 5.6, $|S| = \sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2 + a}{p} \right) \right)$, and in Ex. 5.7. , $|S| = p - 1$ if $p \nmid a$,
 $|S| = 2p - 1$ if $p \mid a$.

So

$$|S| - p = \sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p} \right) = \begin{cases} -1 & \text{if } p \nmid a \\ p - 1 & \text{if } p \mid a \end{cases}$$

□

Ex. 5.9 Prove that $1^2 3^2 \dots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$ using Wilson's theorem.

Proof. Here p is an odd prime.

From Wilson's theorem, as $k(p-k) \equiv -k^2 \pmod{p}$ for $k = 1, 2, \dots, p-1$,

$$\begin{aligned} -1 &\equiv (p-1)! \\ &\equiv \left[1 \times 2 \times \dots \times k \times \dots \times \left(\frac{p-1}{2} \right) \right] \times \left[\left(\frac{p+1}{2} \right) \times \dots \times (p-k) \dots \times (p-2) \times (p-1) \right] \\ &\equiv \prod_{k=1}^{(p-1)/2} k(p-k) \\ &\equiv (-1)^{(p-1)/2} \prod_{k=1}^{(p-1)/2} k^2 \\ &\equiv (-1)^{(p-1)/2} \left[\left(\frac{p-1}{2} \right)! \right]^2 \pmod{p} \end{aligned}$$

So

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

Moreover, from Wilson' theorem and Fermat's little theorem,

$$\begin{aligned} 1^2 2^2 3^2 \dots (p-1)^2 &= [(p-1)!]^2 \equiv 1 \pmod{p} \\ 2^2 4^2 \dots (p-1)^2 &= (2^{p-1})^2 \left[\left(\frac{p-1}{2} \right)! \right]^2 \equiv \left[\left(\frac{p-1}{2} \right)! \right]^2 \pmod{p} \end{aligned}$$

Thus

$$1^2 3^2 \dots (p-2)^2 \left[\left(\frac{p-1}{2} \right)! \right]^2 \equiv 1 \pmod{p},$$

which gives

$$1^2 3^2 \dots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

□

Ex. 5.10 Let $r_1, r_2, \dots, r_{(p-1)/2}$ be the quadratic residues between 1 and p . Show that their product is congruent to 1 (mod p) if $p \equiv 3 \pmod{4}$, and to -1 if $p \equiv 1 \pmod{4}$.

Proof. We proved in Ex. 5.9 that

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

The application $f : \left\{ \begin{array}{ccc} \{\bar{1}, \bar{2}, \dots, \overline{(p-1)/2}\} & \mapsto & \{\bar{r}_1, \bar{r}_2, \dots, \overline{r_{(p-1)/2}}\} \\ x & \mapsto & x^2 \end{array} \right.$ is a bijection, so

$$\prod_{i=1}^{(p-1)/2} r_i \equiv \left[\left(\frac{p-1}{2} \right)! \right]^2 \pmod{p},$$

so

$$\prod_{i=1}^{(p-1)/2} r_i \equiv (-1)^{(p+1)/2} \pmod{p}.$$

That is to say, the product of the quadratic residues between 1 and p is congruent to 1 (mod p) if $p \equiv 3 \pmod{4}$, and to -1 if $p \equiv 1 \pmod{4}$. □

Ex. 5.11 Suppose that $p \equiv 3 \pmod{4}$, and that $q = 2p + 1$ is also prime. Prove that $2^p - 1$ is not prime. (Hint : Use the quadratic character of 2 to show that $q \mid 2^p - 1$) One must assume that $p > 3$.

Proof. The result is false if $p = 3$, so we must suppose $p > 3$.

$p = 4k + 3$ for an integer k , so $q = 2p + 1 = 8k + 7 \equiv -1 \pmod{8}$. Thus

$$\left(\frac{2}{q} \right) = (-1)^{(q^2-1)/8} = 1.$$

So $2^{(q-1)/2} \equiv 1 \pmod{q}$, $2^p \equiv 1 \pmod{q}$, so $q \mid 2^p - 1$.

Moreover, as $p > 3$, $q = 2p + 1 < 2^p - 1$

$$(2p + 1 < 2^p - 1 \iff 2p < 2^p - 2 \iff p + 1 < 2^{p-1}.$$

$4 + 1 < 2^{4-1}$ and for all $k \geq 4$, $k + 1 < 2^{k-1}$ implies $k + 2 < 2^{k-1} + 1 \leq 2^k$, and $4 + 1 < 2^{4-1}$, so by induction $k + 1 < 2^{k-1}$ for all $k > 3$.

So $q \mid 2^p - 1$ with $1 < q < 2^p - 1$: $2^p - 1$ is composite.

Conclusion : if $p \equiv 3 \pmod{4}$, $p > 3$ is prime, and $q = 2p + 1$ is also prime, then $2^p - 1$ is not a prime.

For instance, le Mersenne's number $2^{11} - 1 = 2047$ is not a prime : $2047 = 23 \times 89$. □

Ex. 5.12 Let $f(x) \in \mathbb{Z}[x]$. We say that a prime p divides $f(x)$ if there's an integer n such that $p \mid f(n)$. Describe the prime divisors of $x^2 + 1$ and $x^2 - 2$.

Proof. p divides $x^2 + 1$ iff there exists $a \in \mathbb{Z}$ such that $-1 \equiv a^2 \pmod{p}$, iff $p = 2$ or $\left(\frac{-1}{p}\right) = 1$ iff $p = 2$ or $p \equiv 1 \pmod{4}$.

p divides $x^2 - 2$ iff there exists $a \in \mathbb{Z}$ such that $2 \equiv a^2 \pmod{p}$, iff $p = 2$ or $\left(\frac{2}{p}\right) = 1$ iff $p = 2$ or $p \equiv \pm 1 \pmod{8}$. \square

Ex. 5.13 Show that any prime divisor of $x^4 - x^2 + 1$ is congruent to 1 modulo 12.

Proof. • As $a^6 + 1 = (a^2 + 1)(a^4 - a^2 + 1)$, $p \mid a^4 - a^2 + 1$ implies $p \mid a^6 + 1$, so $\left(\frac{-1}{p}\right) = 1$ and $p \equiv 1 \pmod{4}$.

• $p \mid 4a^4 - 4a^2 + 4 = (2a - 1)^2 + 3$, so $\left(\frac{-3}{p}\right) = 1$.

As $-3 \equiv 1 \pmod{4}$, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$, so $\left(\frac{p}{3}\right) = 1$, thus $p \equiv 1 \pmod{3}$.

$4 \mid p - 1$ and $3 \mid p - 1$, thus $12 \mid p - 1$:

$$p \equiv 1 \pmod{12}.$$

\square

Ex. 5.14 Use the fact that $U(\mathbb{Z}/p\mathbb{Z})$ is cyclic to give a direct proof that $\left(\frac{-3}{p}\right) = 1$ when $p \equiv 1 \pmod{3}$. [Hint : There is a ρ in $U(\mathbb{Z}/p\mathbb{Z})$ of order 3. Show that $(2\rho + 1)^2 = -3$.]

Proof. Suppose that $p \equiv 1 \pmod{3}$. Let g a generator of \mathbb{F}_p^* . Then g has order $p - 1$, thus $\rho = g^{(p-1)/3}$ has order 3. As $\rho^3 = 1, \rho \neq 1$, then $\rho^2 + \rho + 1 = 0$.

$$\begin{aligned} (2\rho + 1)^2 &= 4\rho^2 + 4\rho + 1 \\ &= 4(\rho^2 + \rho + 1) - 3 \\ &= -3. \end{aligned}$$

Thus $\left(\frac{-3}{p}\right) = 1$. \square

The converse is also true for an odd prime p : if $\left(\frac{-3}{p}\right) = 1$, then there exists $a \in \mathbb{F}_p^*$ such that $-\bar{3} = a^2$. $\rho = \frac{-1+a}{2}$ has order 3. Indeed $\rho^2 = \frac{1+a^2-2a}{4} = \frac{-2-2a}{4} = \frac{-1-a}{2}$, so

$$\begin{aligned} 1 + \rho + \rho^2 &= 1 + \frac{-1+a}{2} + \frac{-1-a}{2} \\ &= 0 \end{aligned}$$

so $\rho \neq 1, \rho^3 = 1$. The group \mathbb{F}_p^* contains an element of order 3, thus from Lagrange's theorem $3 \mid p - 1$: $p \equiv 1 \pmod{3}$.

Ex. 5.15 If $p \equiv 1 \pmod{5}$, show directly that $\left(\frac{5}{p}\right) = 1$ by the method of Ex. 5.14. [Hint : Let ρ be an element of $U(\mathbb{Z}/p\mathbb{Z})$ of order 5. Show that $(\rho + \rho^4)^2 + (\rho + \rho^4) - \bar{1} = \bar{0}$, etc.]

Proof. Let g a generator of \mathbb{F}_p^* . g has order $p-1$, thus $\rho = g^{(p-1)/5}$ has order 5.

Let

$$\begin{cases} \alpha &= \rho + \rho^4 \\ \beta &= \rho^2 + \rho^3 \end{cases}$$

As $0 = \rho^5 - 1 = (\rho - 1)(1 + \rho + \rho^2 + \rho^3 + \rho^4)$ and $\rho \neq 1$, then $1 + \rho + \rho^2 + \rho^3 + \rho^4 = 0$, thus

$$\begin{aligned} \alpha + \beta &= -1 \\ \alpha\beta &= \rho^3 + \rho^4 + \rho + \rho^2 = -1 \end{aligned}$$

So α, β are the roots in \mathbb{F}_p of $x^2 + x - 1 : \alpha^2 + \alpha - 1 = 0$.

Thus $4\alpha^2 + 4\alpha - 4 = (2\alpha + 1)^2 - 5 = 0 : 5$ is a square in \mathbb{F}_p^* and $\left(\frac{5}{p}\right) = 1$. \square

Ex. 5.16 Using quadratic reciprocity find the primes for which 7 is quadratic residue. Do the same for 15.

Proof. 7 is a quadratic residue for 2 and for the odd primes such that $\left(\frac{7}{p}\right) = 1$.

From the law of quadratic reciprocity,

$$\left(\frac{7}{p}\right) = 1 \iff (-1)^{(p-1)/2} \left(\frac{p}{7}\right) = 1$$

iff either $p \equiv 1 \pmod{4}$ and $\left(\frac{p}{7}\right) = 1$, or $p \equiv -1 \pmod{4}$ and $\left(\frac{p}{7}\right) = -1$.

In the first case, $p \equiv 1 \pmod{4}, p \equiv 1, 4, 2 \pmod{7}$, which gives $p \equiv 1, -3, 9 \pmod{28}$.

In the second case, $p \equiv -1 \pmod{4}, p \equiv -1, -4, -2 \pmod{7}$, which gives $p \equiv -1, 3, -9 \pmod{28}$.

Conclusion : the primes for which 7 is a quadratic residue are 2 and the odd primes p such that

$$\left(\frac{7}{p}\right) = 1 \iff p \equiv \pm 1, \pm 3, \pm 9 \pmod{28}.$$

\square

15 is a quadratic residue for 2 and for the odd primes such that $\left(\frac{15}{p}\right) = 1$.

$$\left(\frac{15}{p}\right) = 1 \iff \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = 1 \text{ or } \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = -1$$

From the examples of theorem 2, we know that

$$\left(\frac{3}{p}\right) = 1 \iff p \equiv 1, -1 \pmod{12}, \quad \left(\frac{3}{p}\right) = -1 \iff p \equiv 5, -5 \pmod{12},$$

$$\left(\frac{5}{p}\right) = 1 \iff p \equiv 1, -1 \pmod{5}, \quad \left(\frac{5}{p}\right) = -1 \iff p \equiv 2, -2 \pmod{5}.$$

As $5 \wedge 12 = 1$, there exist 8 cases, all possible, which give

$$\left(\frac{15}{p}\right) = 1 \iff p \equiv \pm 1, \pm 7, \pm 11, \pm 17 \pmod{60}.$$

For instance, the primes 2, 7, 11, 17, 43, 53, 59, 61, 67, 137, ... are suitable.

Ex. 5.17 Supply the details to the proof of Proposition 5.2.1 and to the corollary to the lemma following it.

Proposition 5.2.1

(a) $(a_1/b) = (a_2/b)$ if $a_1 \equiv a_2 \pmod{b}$.

(b) $(a_1 a_2/b) = (a_1/b)(a_2/b)$.

(c) $(a/b_1 b_2) = (a/b_1)(a/b_2)$.

Proof. (a) Let $b = p_1 p_2 \cdots p_m$, where the p_i are not necessarily distinct primes. For each prime p_i , $(a_1, p_i) = (a_2, p_i)$ (Prop. 5.1.2 (c)), so $\prod_i (a_1, p_i) = \prod_i (a_2, p_i)$, thus $(a_1/b) = (a_2/b)$.

(b) From Prop. 5.1.2(b),

$$(a_1 a_2/b) = \prod_i (a_1 a_2/p_i) = \prod_i (a_1/p_i)(a_2/p_i) = \prod_i (a_1/p_i) \prod_i (a_2/p_i) = (a_1/b)(a_2/b).$$

(c) Let $b_1 = p_1 p_2 \cdots p_m$, $b_2 = q_1 q_2 \cdots q_l$. Then $b_1 b_2 = p_1 p_2 \cdots p_m q_1 q_2 \cdots q_l = \prod_{i=1}^{m+l} r_i$, where $r_i = p_i$ for $i = 1, \dots, m$, $r_i = q_{i-m}$ for $i = m+1, \dots, m+l$. Then

$$(a/b_1 b_2) = \prod_{i=1}^{m+l} (a/r_i) = \prod_{i=1}^m (a/p_i) \prod_{j=1}^l (a/q_j) = (a/b_1)(a/b_2).$$

□

Lemma. Let r and s be odd integers. Then

(a) $(rs - 1)/2 \equiv ((r - 1)/2) + ((s - 1)/2) \pmod{2}$.

(b) $(r^2 s^2 - 1)/8 \equiv ((r^2 - 1)/8) + ((s^2 - 1)/8) \pmod{2}$.

(Proof in the book.)

Corollary. Let r_1, r_2, \dots, r_m be odd integers. Then

(a) $\sum_{i=1}^m (r_i - 1)/2 \equiv (r_1 r_2 \cdots r_m - 1)/2 \pmod{2}$.

(b) $\sum_{i=1}^m (r_i^2 - 1)/8 \equiv (r_1^2 r_2^2 \cdots r_m^2 - 1)/8 \pmod{2}$.

Proof. Let $\mathcal{P}(m)$ the proposition defined by

$$\mathcal{P}(m) \iff \sum_{i=1}^m (r_i - 1)/2 \equiv (r_1 r_2 \cdots r_m - 1)/2 \pmod{2}.$$

Then $\mathcal{P}(1) \iff (r_1 - 1)/2 \equiv (r_1 - 1)/2 \pmod{2}$ is true, and $\mathcal{P}(2)$ is part (a) of the lemma. If we make the induction hypothesis $\mathcal{P}(m)$, then

$$\begin{aligned} \sum_{i=1}^{m+1} (r_i - 1)/2 &= \sum_{i=1}^m (r_i - 1)/2 + (r_{m+1} - 1)/2 \\ &\equiv (r_1 r_2 \cdots r_m - 1)/2 + (r_{m+1} - 1)/2 \pmod{2} \\ &\equiv (r_1 r_2 \cdots r_m r_{m+1} - 1)/2 \pmod{2}, \end{aligned}$$

where the last congruence is a consequence of the part (a) of the Lemma : the induction is completed, and $\mathcal{P}(m)$ is true for all $m \geq 1$.

The proof of part (b) is similar. □

Ex. 5.18 Let D be a square-free integer that is also odd and positive. Show that there is an integer b prime to D such that $(b/D) = -1$.

Proof. Let $D = p_1 p_2 \cdots p_k$, where the p_i are distinct odd primes.

Let s a nonresidue modulo p_k . From Chinese remainder theorem, as $p_i \wedge p_j = 1$ if $i \neq j$, there exists an integer b such that

$$b \equiv 1 \pmod{p_1}, b \equiv 1 \pmod{p_2}, \dots, b \equiv 1 \pmod{p_{k-1}}, b \equiv s \pmod{p_k}.$$

Then $(b/p_i) = 1$, $i = 1, 2, \dots, k-1$, $(b/p_k) = -1$, so $b \wedge p_i = 1$ for all $i = 1, 2, \dots, k$. Then $b \wedge D = b \wedge p_1 \cdots p_k = 1$, and

$$\left(\frac{b}{D}\right) = \prod_{i=1}^k \left(\frac{b}{p_i}\right) = \left(\frac{b}{p_k}\right) = -1.$$

□

Ex. 5.19 Let D be as in Exercise 18. Show that $\sum(a/D) = 0$, where the sum is over a reduced residue system modulo D . Conclude that exactly one half of the elements in $U(\mathbb{Z}/D\mathbb{Z})$ satisfy $(a/D) = 1$.

Proof. Let b such that $(b/D) = -1$ and $b \wedge D = 1$: the existence of b comes from Ex 5.18.

Let $S = \sum_{a \in A} (a/D)$, where A is reduced residue system modulo D . As two reduced system modulo D represent the same elements in $U(\mathbb{Z}/D\mathbb{Z})$, the sum is independent of the reduced residue system A : we can write

$$S = \sum_{\bar{a} \in U(\mathbb{Z}/D\mathbb{Z})} (a/D).$$

As $b \wedge D = 1$, we know from Ex. 3.6 that $B = bA = \{ba \mid a \in A\}$ is also a reduced system modulo D . In other words, the application $U(\mathbb{Z}/D\mathbb{Z}) \rightarrow U(\mathbb{Z}/D\mathbb{Z}), \bar{a} \mapsto \bar{a}\bar{b}$ is a bijection, so

$$\left(\frac{b}{D}\right) S = \sum_{\bar{a} \in U(\mathbb{Z}/D\mathbb{Z})} \left(\frac{b}{D}\right) \left(\frac{a}{D}\right) = \sum_{\bar{a} \in U(\mathbb{Z}/D\mathbb{Z})} \left(\frac{ba}{D}\right) = \sum_{\bar{c} \in U(\mathbb{Z}/D\mathbb{Z})} \left(\frac{c}{D}\right) = S \quad (\bar{c} = \bar{a}\bar{b}).$$

As $(b/D) = -1$, $-S = S$, so $S = 0$.

Since $(a/D) = \pm 1$, one half of the elements in $U(\mathbb{Z}/D\mathbb{Z})$ satisfy $(a/D) = 1$, and one half of the elements in $U(\mathbb{Z}/D\mathbb{Z})$ satisfy $(a/D) = -1$. □

Ex. 5.20 (continuation) Let $a_1, a_2, \dots, a_{\phi(D)/2}$ be integers between 1 and D such that $(a_i, D) = 1$ and $(a_i/D) = 1$. Prove that D is a quadratic residue modulo a prime $p \nmid D$, $p \equiv 1 \pmod{4}$ iff $p \equiv a_i \pmod{D}$ for some i .

Proof. From Ex. 5.19 we know that there exist exactly $\phi(D)/2$ integers a_i between 1 and D such that $a_i \wedge D = 1$ and $(a_i/D) = 1$. So $\{\bar{a}_1, \dots, \bar{a}_{\phi(D)/2}\}$ is the set of all $\bar{a} \in U(\mathbb{Z}/D\mathbb{Z})$ such that $(a/D) = 1$.

Let $D = p_1 p_2 \cdots p_k$, with distinct p_i , and p a prime number, $p \equiv 1 \pmod{4}$, $p \notin \{p_1, \dots, p_k\}$ (so $p = 4k + 1$, $k \in \mathbb{N}$).

(\Leftarrow) Suppose that $p \equiv a_i$ for some i , $1 \leq i \leq \phi(D)/2$, then $(p/D) = (a_i/D) = 1$, so (Prop. 5.2.2)

$$\left(\frac{D}{p}\right) = (-1)^{\frac{p-1}{2} \frac{D-1}{2}} \left(\frac{p}{D}\right) = (-1)^{2k(\frac{D-1}{2})} \left(\frac{p}{D}\right) = \left(\frac{p}{D}\right) = 1.$$

(\Rightarrow) Suppose that D is a quadratic residue modulo p . Then $(D/p) = 1$, so

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

Thus $\bar{p} \in \{\bar{a}_1, \dots, \bar{a}_{\phi(D)/2}\}$ since $\{\bar{a}_1, \dots, \bar{a}_{\phi(D)/2}\}$ is the set of all $\bar{a} \in U(\mathbb{Z}/D\mathbb{Z})$ such that $(a/D) = 1$. Consequently $p \equiv a_i \pmod{D}$ for some i . \square

Ex. 5.21 Apply the method of Ex. 5.19 and 5.20 to find those primes for which 21 is a quadratic residue.

Proof. Let $D = 21 = 3 \times 7$ (D is positive, odd and square-free). We first search the $\phi(D)/2 = 6$ integers a , $1 \leq a \leq 21$, such that $(a/D) = 1$.

$$\left(\frac{a}{21}\right) = 1 \iff \left(\frac{a}{3}\right) = \left(\frac{a}{7}\right) = 1 \text{ or } \left(\frac{a}{3}\right) = \left(\frac{a}{7}\right) = -1.$$

The first case is equivalent to $a \equiv 1 \pmod{3}$, $a \equiv 1, 2, 4 \pmod{7}$, that is $a \equiv 1, 16, 4 \pmod{21}$.

The second case gives $a \equiv -1 \pmod{3}$, $a \equiv -1, -2, -4 \pmod{7}$, that is $a \equiv -1, -16, -4 \pmod{21}$, or equivalently $a \equiv 20, 5, 17 \pmod{21}$.

So $A = \{1, 4, 5, 16, 17, 20\}$ is the set of the integers a such that $1 \leq a \leq 21$, $(a/D) = 1$.

As $(21/3) = (21/7) = 0$, 21 is not a quadratic residue modulo 3 or 7.

• $p \equiv 1 \pmod{4}$.

From Ex.5.20, we know that $D = 21$ is a quadratic residue modulo an odd prime p , $p \neq 3, p \neq 7$, $p \equiv 1 \pmod{4}$, iff $p \equiv a \pmod{D}$ for some $a \in A$.

• $p \equiv -1 \pmod{4}$.

As $D = 21 \equiv 1 \pmod{4}$, $\left(\frac{D}{p}\right) \left(\frac{p}{D}\right) = (-1)^{\frac{p-1}{2} \frac{D-1}{2}} = 1$, so the same reasoning as in Ex. 5.20 show that D is a quadratic residue modulo 21 iff $p \equiv a, a \in A$.

Conclusion : 21 is a quadratic residue for 2, and for the primes p such that

$$p \equiv 1, 4, 5, 16, 17, 20 \pmod{21}.$$

\square

Ex. 5.22 Use the Jacobi symbol to determine $(113/997)$, $(215/761)$, $(514/1093)$, and $(401/757)$.

Proof. $(113/997) = (997/113) = (93/113) = (113/93) = (20/93) = (2^2/93)(5/93) = (5/93) = (93/5) = (3/5) = (5/3) = (2/3) = -1$.

$(215/761) = (761/215) = (116/215) = (2^2/215)(29/215) = (29/215) = (215/29) = (12/29) = (2^2/29)(3/29) = (3/29) = (29/3) = (2/3) = -1$.

$(514/1093) = (2/1093)(257/1093) = -(257/1093) = -(1093/57) = -(65/257) = -(257/65) = -(62/65) = -(2/65)(31/65) = -(31/65) = -(65/31) = -(3/31) = (31/3) = (1/3) = 1$.

$(401/757) = (757/401) = (356/401) = (401/89) = (45/89) = (89/45) = (44/45) = (2^2/45)(11/45) = (11/45) = (45/11) = (1/11) = 1$. \square

Ex. 5.23 Suppose that $p \equiv 1 \pmod{4}$. Show that there exist integers s and t such that $pt = 1 + s^2$. Conclude that p is not a prime in $\mathbb{Z}[i]$. Remember that $\mathbb{Z}[i]$ has unique factorization.

Proof. As $p \equiv 1 \pmod{4}$, then $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$: -1 is a square modulo p .

So $-1 \equiv s^2 \pmod{p}$, $s \in \mathbb{Z}$: there exist $s \in \mathbb{Z}, t \in \mathbb{Z}$ such that $pt = 1 + s^2$.

In $\mathbb{Z}[i]$, $p \mid (s+i)(s-i)$.

If p was a prime in $\mathbb{Z}[i]$, then $p \mid s+i$ ou $p \mid s-i$.

This implies $s \pm i = (a+bi)p$, $(a,b) \in \mathbb{Z}^2$, thus $\pm 1 = bp$, $p \mid 1$: it's impossible.

Conclusion : if $p \equiv 1 \pmod{4}$, p is not a prime in $\mathbb{Z}[i]$. \square

Ex. 5.24 If $p \equiv 1 \pmod{4}$, show that p is a sum of two squares, i.e. $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$. (Hint : $p = \alpha\beta$, with α and β being non units in $\mathbb{Z}[i]$. Remember that $\mathbb{Z}[i]$ has unique factorisation.)

Proof. $\mathbb{Z}[i]$ is a principal ideal domain, thus p prime is in $\mathbb{Z}[i]$ iff p is irreducible in $\mathbb{Z}[i]$.

If $p \equiv 1 \pmod{4}$, p is not a prime from Ex.5.23, so it is not irreducible :

$p = \alpha\beta$, $\alpha, \beta \in \mathbb{Z}[i]$, $N(\alpha) > 1$, $N(\beta) > 1$ (where $N(a+bi) = a^2 + b^2$ is the complex norm).

$N(p) = p^2 = N(u)N(v)$, $1 < N(u) < p^2$

Thus $N(u) = p$, that is $p = a^2 + b^2$, where $u = a+bi$.

Conclusion : if p is prime in \mathbb{N} , $p \equiv 1 \pmod{4}$, then $p = a^2 + b^2$, $a, b \in \mathbb{Z}$, p is a sum of two squares. \square

Ex. 5.25 An integer is called a biquadratic residue modulo p if it is congruent to a fourth power. Using the identity $x^4 + 4 = ((x+1)^2 + 1)((x-1)^2 + 1)$ show that -4 is a biquadratic residue modulo p iff $p \equiv 1 \pmod{4}$.

Proof. $x^4 + 4 = (x^4 + 4x^2 + 4) - 4x^2 = (x^2 + 2)^2 - 4x^2 = (x^2 + 2 - 2x)(x^2 + 2 + 2x)$, so

$$x^4 + 4 = ((x-1)^2 + 1)((x+1)^2 + 1).$$

If $-4 \equiv x^4 \pmod{p}$, then $p \mid (x+1)^2 + 1$ or $p \mid (x-1)^2 + 1$

In the two cases, -1 is a quadratic residue modulo p , thus $\left(\frac{-1}{p}\right) = 1$: $p \equiv 1 \pmod{4}$.

Conversely, if $p \equiv 1 \pmod{4}$, $\left(\frac{-1}{p}\right) = 1$, then it exists an integer a such that $-1 \equiv a^2 \pmod{p}$.

Let $x = a - 1$. Then $p \mid (x+1)^2 + 1$, thus $p \mid x^4 + 4$: -4 is a biquadratic residue modulo p .

Conclusion :

$$\exists x \in \mathbb{Z}, x^4 \equiv -4 \pmod{p} \iff p \equiv 1 \pmod{4}.$$

\square

Ex. 5.26 This exercise and Ex. 5.27 and 5.28 give Dirichlet's beautiful proof that 2 is a biquadratic residue modulo p iff p can be written in the form $A^2 + 64B^2$, where $A, B \in \mathbb{Z}$. Suppose that $p \equiv 1 \pmod{4}$. Then $p = a^2 + b^2$ by Ex. 5.24. Take a to be odd. Prove the following statements:

(a) $(a/p) = 1$.

(b) $((a+b)/p) = (-1)^{((a+b)^2-1)/8}$.

$$(c) \ (a+b)^2 \equiv 2ab \pmod{p}$$

$$(d) \ (a+b)^{(p-1)/2} \equiv (2ab)^{(p-1)/4} \pmod{p}.$$

Proof. Let p a prime number, $p \equiv 1 \pmod{4} : p = 4k + 1, k \in \mathbb{N}^*$.

Then $p = a^2 + b^2$ (Ex. 5.24).

As a, b are not of the same parity, up to exchange a and b , we will suppose that a is odd (then b is even).

(a)

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = a^{2k} \pmod{p}.$$

Using the law of quadratic reciprocity for Jacobi's symbol (Proposition 5.2.2), where a, p are odd numbers :

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

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

If $a = p_1 p_2 \cdots p_l$ is the decomposition of a in prime factors, with not necessarily distinct primes , then

$$\left(\frac{p}{a}\right) = \left(\frac{p}{p_1}\right) \left(\frac{p}{p_2}\right) \cdots \left(\frac{p}{p_l}\right).$$

Since $p = a^2 + b^2$, $p \equiv b^2 \pmod{p_i}$, thus $\left(\frac{p}{p_i}\right) = 1$ for all i .

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = 1.$$

(b) $a + b$ is odd, and $p \equiv 1 \pmod{4}$, thus

$$\left(\frac{a+b}{p}\right) = \left(\frac{p}{a+b}\right) = \left(\frac{2^2 p}{a+b}\right) = \left(\frac{2}{a+b}\right) \left(\frac{2p}{a+b}\right).$$

If $a + b = q_1 q_2 \cdots q_l$, as $2p = (a+b)^2 + (a-b)^2$, $2p \equiv (a-b)^2 \pmod{q_i}$, thus $\left(\frac{2p}{q_i}\right) = 1$.

$$\left(\frac{2p}{a+b}\right) = \left(\frac{2p}{q_1}\right) \cdots \left(\frac{2p}{q_l}\right) = 1.$$

Moreover $\left(\frac{2}{a+b}\right) = (-1)^{\frac{(a+b)^2-1}{8}}$, so

$$\left(\frac{a+b}{p}\right) = (-1)^{\frac{(a+b)^2-1}{8}}.$$

$$(c) \ (a+b)^2 = a^2 + b^2 + 2ab = p + 2ab \equiv 2ab \pmod{p}$$

$$(d) [(a+b)^2]^{\frac{p-1}{4}} \equiv (2ab)^{\frac{p-1}{4}} \pmod{p}, \text{ thus}$$

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

□

Ex. 5.27 Suppose that f is such that $b \equiv af \pmod{p}$. Show that $f^2 \equiv -1 \pmod{p}$, and that $2^{(p-1)/4} \equiv f^{ab/2} \pmod{p}$.

Proof. Let f such as $b \equiv af \pmod{p}$.

This is equivalent to $\bar{f} = \bar{b}\bar{a}^{-1}$ in \mathbb{F}_p^* .

As $\bar{a}^2 = -\bar{b}^2$, $\bar{f}^2 = -1$: $f^2 \equiv -1 \pmod{p}$.

We deduce from Ex. 5.26 (d) and (b) that

$$\begin{aligned} (2ab)^{\frac{p-1}{4}} &\equiv (a+b)^{\frac{p-1}{2}} = \left(\frac{a+b}{p}\right) \\ &\equiv (-1)^{\frac{(a+b)^2-1}{8}} \\ &\equiv (f^2)^{\frac{(a+b)^2-1}{8}} \\ &\equiv f^{\frac{(a+b)^2-1}{4}} = f^{\frac{a^2+b^2-1+2ab}{4}} \\ &\equiv f^{\frac{p-1}{4}} f^{\frac{ab}{2}} \pmod{p} \end{aligned}$$

Since $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) = 1$ from Ex. 5.26(a)), then

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

so

$$2^{\frac{p-1}{4}} f^{\frac{p-1}{4}} \equiv f^{\frac{ab}{2}} f^{\frac{p-1}{4}} \pmod{p}.$$

As $f^{\frac{p-1}{4}} \not\equiv 0 \pmod{p}$,

$$2^{\frac{p-1}{4}} \equiv f^{\frac{ab}{2}} \pmod{p}.$$

□

Ex. 5.28 Show that $x^4 \equiv 2 \pmod{p}$ has a solution for $p \equiv 1 \pmod{4}$ iff p is of the form $A^2 + 64B^2$.

Proof. If $p \equiv 1 \pmod{4}$ and if there exists $x \in \mathbb{Z}$ such that $x^4 \equiv 2 \pmod{p}$, then

$$2^{\frac{p-1}{4}} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

From Ex. 5.27, where $p = a^2 + b^2$, a odd, we know that

$$f^{\frac{ab}{2}} \equiv 2^{\frac{p-1}{4}} \equiv 1 \pmod{p}.$$

Since $f^2 \equiv -1 \pmod{p}$, the order of f modulo p is 4, thus $4 \mid \frac{ab}{2}$, so $8 \mid ab$.

As a is odd, $8 \mid b$, then $p = A^2 + 64B^2$ (with $A = a$, $B = b/8$).

Conversely, if $p = A^2 + 64B^2$, then $p \equiv 1 \pmod{4}$.

Let $a = A$, $b = 8B$. Then

$$2^{\frac{p-1}{4}} \equiv f^{\frac{ab}{2}} \equiv f^{4AB} \equiv (-1)^{2AB} \equiv 1 \pmod{p}.$$

As $2^{\frac{p-1}{4}} \equiv 1 \pmod{p}$, $x^4 \equiv 2 \pmod{p}$ has a solution in \mathbb{Z} (Prop. 4.2.1) : 2 is a biquadratic residue modulo p .

Conclusion :

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

Note : the equation $x^4 \equiv 2 \pmod{p}$ has also solutions if $p \equiv -1 \pmod{8}$.

Indeed, the equation $x^4 \equiv 2 \pmod{p}$ has a solution in \mathbb{Z} iff $2^{\frac{p-1}{d}} \equiv 1$, where $d = 4 \wedge (p-1) = 2$, thus iff $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, which is true since $\left(\frac{2}{p}\right) = 1$.

For instance, $8^4 \equiv 2 \pmod{23}$, with $23 \equiv -1 \pmod{8}$. □

Ex. 5.29 Let (RR) be the number of pairs $(n, n+1)$ in the set $1, 2, 3, \dots, p-1$ such that n and $n+1$ are both quadratic residues modulo p . Let (NR) be the number of pairs $(n, n+1)$ in the set $1, 2, 3, \dots, p-1$ such that n is a quadratic nonresidue and $n+1$ is a quadratic residue. Similarly, define (RN) and (NN) . Determine the sums $(RR) + (RN)$, $(NR) + (NN)$, $(RR) + (NR)$, and $(RN) + (NN)$.

Proof. Let E the set of pairs $(n, n+1) \in \mathbb{N}^2, 1 \leq n \leq p-2 : |E| = p-2$.

Write RR the set of pairs $(n, n+1)$ such that n and $n+1$ are both a quadratic residues, and $(RR) = |RR|$ its cardinality, and similar definitions for RN, NR, NN .

As $E = RR \cup RN \cup NR \cup NN$ (disjoint union),

$$(RR) + (RN) + (NR) + (NN) = |E| = p-2.$$

• $RR \cup RN$ is the set of pairs $(n, n+1)$ in E such that n is a residue. Its cardinality is the number of residues in $[1, p-2]$, so the number of residues in $[1, p-1]$, minus s , where $s = 1$ if $p-1$ is a residue, $s = 0$ otherwise. In both cases $p \equiv 1, 3 \pmod{4}$, $s = \frac{1+(-1)^{\frac{p-1}{2}}}{2}$, and the total number of residues is $(p-1)/2$, so

$$(RR) + (RN) = \frac{p-1}{2} - s = \frac{p-1}{2} - \frac{1+(-1)^{\frac{p-1}{2}}}{2} = \frac{1}{2}(p-2 - (-1)^{\frac{p-1}{2}}).$$

• Similarly, $(NR) + (NN)$ is the number of nonresidues in $[1, p-1]$, minus t , where $t = 1$ if $p-1$ is a nonresidue, $t = 0$ otherwise : $t = \frac{1-(-1)^{\frac{p-1}{2}}}{2}$, so

$$(NR) + (NN) = \frac{1}{2}(p-2 + (-1)^{\frac{p-1}{2}})$$

(the sum of these two results is indeed $p-2 = |E|$).

• As 1 is a residue, $(RR) + (NR)$ is the number of residues in $[1, p-1]$, minus 1 :

$$(RR) + (NR) = \frac{p-1}{2} - 1.$$

• $(RN) + (NN)$ is the number of nonresidues in $[2, p-1]$, equal to the number of residues in $[1, p-1]$:

$$(RN) + (NN) = \frac{p-1}{2}.$$

□

Ex. 5.30 Show that $(RR) + (NN) - (RN) - (NR) = \sum_{n=1}^{p-1} (n(n+1)/p)$. Evaluate this sum and show that it is equal to -1 . (Hint : The result of Exercise 8 is useful.)

Proof. Let χ be the characteristic function of $RR \cup NN$: if $1 \leq n \leq p-1$, $\chi(n) = 1$ if $n, n+1$ are both residues, or if $n, n+1$ are both non residues. Then

$$\chi(n) = \frac{1}{2} \left(1 + \left(\frac{n}{p} \right) \left(\frac{n+1}{p} \right) \right)$$

(if $\chi(n) = 1$, $\left(\frac{n}{p} \right) \left(\frac{n+1}{p} \right) = 1$, and $\left(\frac{n}{p} \right) \left(\frac{n+1}{p} \right) = -1$ otherwise.)

Similarly, let χ' the characteristic function of $RN \cup NR$: $\chi'(n) = 1$ if exactly one of the integer $n, n+1$ is a residue, 0 otherwise. Then

$$\chi'(n) = \frac{1}{2} \left(1 - \left(\frac{n}{p} \right) \left(\frac{n+1}{p} \right) \right).$$

As each integer n between 1 and $p-1$ brings the contribution 1 if $n \in RR \cup NN$, and -1 if $n \in RN \cup NR$, then

$$\begin{aligned} (RR) + (NN) - (RN) - (NR) &= \sum_{n=1}^{p-1} (\chi(n) - \chi'(n)) \\ &= \frac{1}{2} \sum_{n=1}^{p-1} \left(1 + \left(\frac{n(n+1)}{p} \right) \right) - \left(1 - \left(\frac{n(n+1)}{p} \right) \right) \\ &= \sum_{n=1}^{p-1} \left(\frac{n(n+1)}{p} \right) \end{aligned}$$

To evaluate this sum S , note that $4n(n+1) = (2n+1)^2 - 1$, so

$$S = \sum_{n=1}^{p-1} \left(\frac{n(n+1)}{p} \right) = \sum_{n=1}^{p-1} \left(\frac{4n(n+1)}{p} \right) = \sum_{n=1}^{p-1} \left(\frac{(2n+1)^2 - 1}{p} \right).$$

This sum can be written $S = \sum_{\bar{n} \in \mathbb{F}_p^*} ((2n+1)^2 - 1)/p = \sum_{\bar{n} \in \mathbb{F}_p} ((2n+1)^2 - 1)/p$, since $(0/p) = 0$. As $f : \mathbb{F}_p \rightarrow \mathbb{F}_p, \bar{n} \mapsto (2\bar{n}+1)$ is a bijection (2 is invertible in \mathbb{F}_p^*),

$$\sum_{\bar{n} \in \mathbb{F}_p} \left(\frac{(2n+1)^2 - 1}{p} \right) = \sum_{\bar{y} \in \mathbb{F}_p} \left(\frac{y^2 - 1}{p} \right) \quad (y = 2n+1).$$

As $p \nmid 1$, the evaluation of this last sum is given in Exercise 5.8 : $S = -1$, so

$$(RR) + (NN) - (RN) - (NR) = \sum_{n=1}^{p-1} \left(\frac{n(n+1)}{p} \right) = -1.$$

□

Ex. 5.31 Use the results of Exercises 29 and 30 to show that $(RR) = \frac{1}{4}(p-4-\varepsilon)$, where $\varepsilon = (-1)^{(p-1)/2}$

Proof. To summarize the results of the Ex. 5.29 and 5.30,

$$\begin{aligned}(a)(RR) + (RN) + (NR) + (NN) &= p - 2 \\ (b)(RR) + (NN) - (RN) - (NR) &= -1\end{aligned}$$

and

$$\begin{aligned}(c)(RR) + (RN) &= \frac{1}{2} \left(p - 2 - (-1)^{\frac{p-1}{2}} \right) \\ (d)(RR) + (NR) &= \frac{p-1}{2} - 1\end{aligned}$$

The sum of (a) and (b) gives

$$(e)(RR) + (NN) = \frac{p-3}{2}.$$

The sum of (c),(d),(e) gives (using (a))

$$2(RR) + p - 2 = \frac{p-2}{2} + \frac{p-1}{2} + \frac{p-3}{2} - 1 - \frac{(-1)^{\frac{p-1}{2}}}{2},$$

so

$$\begin{aligned}2(RR) &= \frac{p-1}{2} + \frac{p-3}{2} - \frac{p-2}{2} - 1 - \frac{(-1)^{\frac{p-1}{2}}}{2} = \frac{p}{2} - 2 - \frac{(-1)^{\frac{p-1}{2}}}{2}, \\ (RR) &= \frac{1}{4}(p - 4 - \varepsilon), \text{ where } \varepsilon = (-1)^{\frac{p-1}{2}}.\end{aligned}$$

□

Ex. 5.32 If p is an odd prime, show that $(2/p) = \prod_{j=1}^{(p-1)/2} 2 \cos(2\pi j/p)$. Use this to give another proof to Proposition 5.1.3.

Proof. Let p an odd prime number, and $\zeta = e^{2i\pi/p}$: then $\zeta^p = 1$.

Let

$$P = \prod_{j=0}^{p-1} (\zeta^j + \zeta^{-j}) = \prod_{j=0}^{p-1} 2 \cos(2\pi j/p).$$

$$\begin{aligned}P &= \zeta^0 \zeta^{-1} \dots \zeta^{-(p-1)} \prod_{j=0}^{p-1} (\zeta^{2j} + 1) \\ &= (\zeta^p)^{-(p-1)/2} \prod_{j=0}^{p-1} (\zeta^{2j} + 1) \\ &= \prod_{j=0}^{p-1} (\zeta^{2j} + 1)\end{aligned}$$

As ζ^j depends only of the class $\bar{j} \in \mathbb{F}_p$, this product can be written

$$P = \prod_{\bar{j} \in \mathbb{F}_p} (\zeta^{2j} + 1) = \prod_{\bar{k} \in \mathbb{F}_p} (\zeta^k + 1) \quad (k = 2j),$$

since $f : \mathbb{F}_p \rightarrow \mathbb{F}_p, x \mapsto 2x$ is a bijection. So

$$P = \prod_{k=0}^{p-1} (\zeta^k + 1).$$

Since $\zeta^0 = 1, \zeta, \dots, \zeta^{p-1}$ are the roots of the polynomial $f(x) = x^p - 1$, then $1 + \zeta^0, \dots, 1 + \zeta^{p-1}$ are the roots of $g(x) = (x - 1)^p - 1 = f(x - 1)$, so $g(x) = \prod_{k=0}^{p-1} (x - (1 + \zeta^k))$.

As $g(0) = (-1)^p - 1 = -2 = (-1 - \zeta^0) \cdots (-1 - \zeta^{p-1}) = -\prod_{k=0}^{p-1} (\zeta^k + 1)$, we obtain

$$P = \prod_{j=0}^{p-1} 2 \cos(2\pi j/p) = \prod_{k=0}^{p-1} (\zeta^k + 1) = 2,$$

so

$$\prod_{j=1}^{p-1} 2 \cos(2\pi j/p) = 1.$$

$$\begin{aligned} 1 &= \prod_{j=1}^{p-1} 2 \cos(2\pi j/p) \\ &= \prod_{j=1}^{(p-1)/2} 2 \cos(2\pi j/p) \prod_{j=(p+1)/2}^{p-1} 2 \cos(2\pi j/p) \\ &= \prod_{j=1}^{(p-1)/2} 2 \cos(2\pi j/p) \prod_{k=1}^{(p-1)/2} 2 \cos(2\pi - 2\pi k/p) \quad (k = p - j) \end{aligned}$$

As $\cos(2\pi - \alpha) = \cos(\alpha)$,

$$1 = \left(\prod_{j=1}^{(p-1)/2} 2 \cos(2\pi j/p) \right)^2, \text{ so } \prod_{j=1}^{(p-1)/2} 2 \cos(2\pi j/p) = \pm 1$$

Case 1 : if $1 \leq j \leq p/4, 0 \leq 2\pi j/p < \pi/2$, so $\cos(2\pi j/p) > 0$,

case 2 : if $p/4 < j \leq (p-1)/2, \pi/2 < 2\pi j/p < \pi$, so $\cos(2\pi j/p) < 0$.

In the first case, $2 \leq 2j \leq (p-1)/2$: the least residue of $2j$ is positive. In the second case $p/2 < 2j \leq p-1$: the least residue of $2j$ is negative.

Let μ the number of negative least residues of the integer $2j$, $1 \leq j \leq (p-1)/2$: we know from Gauss' Lemma that $(2/p) = (-1)^\mu$. As μ is also the number of j , $1 \leq j \leq (p-1)/2$ such that $\cos(2\pi j/p) < 0$,

$$\prod_{j=1}^{(p-1)/2} 2 \cos(2\pi j/p) = (-1)^\mu = \left(\frac{2}{p}\right).$$

If $p \equiv 1 \pmod{8}$, $p = 8q + 1, q \in \mathbb{N}$. For $1 \leq j \leq (p-1)/2$,

$$\cos(2\pi j/p) < 0 \iff p/4 \leq j \leq (p-1)/2 \iff 2q + 1 \leq j \leq 4q,$$

so $\mu = 2q$ and $(2/p) = (-1)^\mu = 1$.

If $p \equiv -1 \pmod{8}$, $p = 8q - 1$, $q \in \mathbb{N}^*$.

$$\cos(2\pi j/p) < 0 \iff p/4 \leq j \leq (p-1)/2 \iff 2q \leq j \leq 4q-1,$$

so $\mu = 2q$ and $(2/p) = (-1)^\mu = 1$.

If $p \equiv 3 \pmod{8}$, $p = 8q + 3$, $q \in \mathbb{N}$.

$$\cos(2\pi j/p) < 0 \iff p/4 \leq j \leq (p-1)/2 \iff 2q+1 \leq j \leq 4q+1,$$

so $\mu = 2q+1$ and $(2/p) = (-1)^\mu = 1$.

If $p \equiv -3 \pmod{8}$, $p = 8q - 3$, $q \in \mathbb{N}^*$,

$$\cos(2\pi j/p) < 0 \iff p/4 \leq j \leq (p-1)/2 \iff 2q \leq j \leq 4q-2,$$

so $\mu = 2q-1$ and $(2/p) = (-1)^\mu = 1$. □

Ex. 5.33 Use Proposition 5.3.2 to derive the quadratic character of -1 .

Proof. Let $f(z) = e^{2\pi iz} - e^{-2\pi iz}$. If p is an odd prime, $a \in \mathbb{Z}$, and $p \nmid a$, we know from Prop. 5.3.2 that

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{la}{p}\right) = \left(\frac{a}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right).$$

For $a = -1$, as $f(-z) = -f(z)$,

$$\begin{aligned} \left(\frac{-1}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right) &= \prod_{l=1}^{(p-1)/2} f\left(\frac{-l}{p}\right) \\ &= (-1)^{(p-1)/2} \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right) \end{aligned}$$

Moreover $f(z) = 0 \iff e^{4\pi iz} = 1 \iff 4\pi iz = 2ki\pi, k \in \mathbb{Z} \iff z = k/2, k \in \mathbb{Z}$, so, if $l \in \mathbb{Z}$, $f\left(\frac{l}{p}\right) = 0 \iff l/p = k/2, k \in \mathbb{Z} \iff p \mid 2l \iff p \mid l$. For $1 \leq l < p$, this is impossible, so $\prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right) \neq 0$. Consequently,

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

□

Ex. 5.34 If p is an odd prime distinct from 3, show that

$$\left(\frac{3}{p}\right) = \prod_{j=1}^{(p-1)/2} \left(3 - 4\sin^2\left(\frac{2\pi j}{p}\right)\right).$$

Proof. Let p an odd prime number, $p \neq 3$ and $\zeta = e^{2i\pi/p}$.

$$\begin{aligned} 3 - 4 \sin^2 \left(\frac{2\pi j}{p} \right) &= 3 - 4 \left(\frac{\zeta^j - \zeta^{-j}}{2i} \right)^2 \\ &= 3 + \zeta^{2j} + \zeta^{-2j} - 2 \\ &= 1 + \zeta^{2j} + \zeta^{-2j} \\ &= 1 + 2 \cos \left(\frac{4\pi j}{p} \right) \end{aligned}$$

(As $\cos(2\alpha) = 1 - 2 \sin^2 \alpha$, so $3 - 4 \sin^2 \alpha = 1 + 2 \cos \alpha$.)

Let

$$P = \prod_{j=1}^{p-1} \left(3 - 4 \sin^2 \left(\frac{2\pi j}{p} \right) \right) = \prod_{\bar{j} \in \mathbb{F}_p^*} \left(3 - 4 \sin^2 \left(\frac{2\pi j}{p} \right) \right).$$

Then

$$\begin{aligned} P &= \prod_{\bar{j} \in \mathbb{F}_p^*} (1 + \zeta^{2j} + \zeta^{-2j}) \\ &= \prod_{\bar{k} \in \mathbb{F}_p^*} (1 + \zeta^k + \zeta^{-k}) \quad (k = 2j) \end{aligned}$$

since $f : \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*, \bar{j} \mapsto 2\bar{j}$ is a bijection. So

$$\begin{aligned} P &= \prod_{k=1}^{p-1} \zeta^{-k} (1 + \zeta^k + \zeta^{2k}) \\ &= \prod_{k=1}^{p-1} \zeta^{-k} \frac{\prod_{k=1}^{p-1} (1 - \zeta^{3k})}{\prod_{k=1}^{p-1} (1 - \zeta^k)} \end{aligned}$$

$\prod_{k=1}^{p-1} \zeta^{-k} = (\zeta^p)^{-(p-1)/2} = 1$. Moreover, $\prod_{k=1}^{p-1} (1 - \zeta^{3k}) = \prod_{k=1}^{p-1} (1 - \zeta^k)$, since $\bar{k} \mapsto 3\bar{k}$ is a bijection in \mathbb{F}_p^* , so $P = 1$, and consequently

$$\begin{aligned} 1 &= \prod_{j=1}^{p-1} \left(3 - 4 \sin^2 \left(\frac{2\pi j}{p} \right) \right) \\ &= \prod_{j=1}^{(p-1)/2} \left(3 - 4 \sin^2 \left(\frac{2\pi j}{p} \right) \right) \prod_{j=(p+1)/2}^{p-1} \left(3 - 4 \sin^2 \left(\frac{2\pi j}{p} \right) \right) \\ &= \prod_{j=1}^{(p-1)/2} \left(3 - 4 \sin^2 \left(\frac{2\pi j}{p} \right) \right) \prod_{k=1}^{(p-1)/2} \left(3 - 4 \sin^2 \left(\frac{2\pi(k-j)}{p} \right) \right) \quad (k = p-j) \\ &= \left[\prod_{j=1}^{(p-1)/2} \left(3 - 4 \sin^2 \left(\frac{2\pi j}{p} \right) \right) \right]^2 \end{aligned}$$

So $\prod_{j=1}^{(p-1)/2} \left(3 - 4 \sin^2 \left(\frac{2\pi j}{p} \right) \right) = \pm 1$.

Let ν the number of negative factors in this product.

If $1 \leq j \leq (p-1)/2$, then $0 < 4\pi j/p < 2\pi$.

$$\begin{aligned}
1 + 2 \cos \frac{4\pi j}{p} < 0 &\iff \cos \frac{4\pi j}{p} < \cos \frac{2\pi}{3} \\
&\iff \frac{2\pi}{3} < \frac{4\pi j}{p} < \frac{4\pi}{3} \\
&\iff \frac{p}{6} < j < \frac{p}{3} \\
&\iff \frac{p}{2} < 3j < p
\end{aligned}$$

Let μ the number of integers $j, 1 \leq j \leq (p-1)/2$ such that their least remainder is negative. Since $3 \leq 3j \leq 3(p-1)/2$ and $3j \neq p/2$, these j are such that $\frac{p}{2} < 3j < p$, so $\mu = \nu$. Therefore

$$\prod_{j=1}^{(p-1)/2} \left(3 - 4 \sin^2 \left(\frac{2\pi j}{p} \right) \right) = (-1)^\nu = (-1)^\mu = \left(\frac{3}{p} \right).$$

□

Ex. 5.35 Use the preceding exercise to show that 3 is a square modulo p iff p is congruent to 1 or -1 modulo 12.

Proof. We know from Ex. 5.34 that $\nu = \text{Card} \{j \in [1, (p-1)/2] \mid p/2 \leq 3j < p\} = \mu$. Therefore ν is the number of j such that $p/6 \leq j < p/3$, so $\nu = \lfloor p/3 \rfloor - \lfloor p/6 \rfloor$.

If $p = 12k + 1$, $\nu = \lfloor p/3 \rfloor - \lfloor p/6 \rfloor = 4k - 2k = 2k : (3/p) = (-1)^\nu = 1$

If $p = 12k + 5$, $\nu = \lfloor p/3 \rfloor - \lfloor p/6 \rfloor = 4k + 1 - 2k = 2k + 1 : (3/p) = (-1)^\nu = -1$

If $p = 12k - 5$, $\nu = \lfloor p/3 \rfloor - \lfloor p/6 \rfloor = 4k - 2 - (2k - 1) = 2k - 1 : (3/p) = (-1)^\nu = -1$

If $p = 12k - 1$, $\nu = \lfloor p/3 \rfloor - \lfloor p/6 \rfloor = 4k - 1 - (2k - 1) = 2k : (3/p) = (-1)^\nu = 1$

3 is a square modulo p ($p \neq 2, p \neq 3$) iff p is congruent to 1 or -1 modulo 12. □

Ex. 5.36 Show that part (c) of Proposition 5.2.2 is true if a is negative and b is positive (both still odd).

As said by Adam Michalik, the Jacobi symbol $\left(\frac{a}{b}\right)$ only defined for positive b , so the question, which concerns $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)$, $a < 0$ makes no sense.

To give sense to this question, we must substitute the Kronecker symbol to the Jacobi symbol. The Kronecker symbol (not defined in Ireland-Rosen) is the usual extension of Jacobi symbol (see for instance [Henri Cohen] A course in computational algebraic number theory, [Henri Cohen] Number theory (vol. 1), or [Harvey Cohn] Advanced number theory).

We define Kronecker (or Kronecker-Jacobi) symbol $\left(\frac{a}{b}\right)$ for any a and b in \mathbb{Z} in the following way.

(1) If $b = 0$, then $\left(\frac{a}{0}\right) = 1$ if $a = \pm 1$, and $\left(\frac{a}{0}\right) = 0$ otherwise.

(2) For $b \neq 0$, write $b = \prod p$, where the p are not necessarily distinct primes (including 2), or $p = -1$ to take care of the sign. Then we set

$$\left(\frac{a}{b}\right) = \prod \left(\frac{a}{p}\right),$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol defined above for $p > 2$, and where we define

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } a \text{ is even} \\ (-1)^{(a^2-1)/8} & \text{if } a \text{ is odd,} \end{cases}$$

and also

$$\left(\frac{a}{-1}\right) = \begin{cases} 1 & \text{if } a \geq 0 \\ -1 & \text{if } a < 0 \end{cases}$$

Proof. Suppose $a < 0, b > 0$, both odd. Let $a = -A, A > 0, A = p_1 p_2 \cdots p_k$, where the p_i are not necessarily distinct primes. Then

$$\begin{aligned} \left(\frac{a}{b}\right) \left(\frac{b}{a}\right) &= \left(\frac{-A}{b}\right) \left(\frac{b}{-A}\right) \\ \left(\frac{-A}{b}\right) &= \left(\frac{-1}{b}\right) \left(\frac{A}{b}\right) = (-1)^{(b-1)/2} \left(\frac{A}{b}\right) \\ \left(\frac{b}{-A}\right) &= \left(\frac{b}{-1}\right) \left(\frac{b}{p_1}\right) \cdots \left(\frac{b}{p_k}\right) = \left(\frac{b}{A}\right) \end{aligned}$$

so, from Prop. 5.2.2, as A, b are odd and positive,

$$\begin{aligned} \left(\frac{a}{b}\right) \left(\frac{b}{a}\right) &= (-1)^{\frac{b-1}{2}} \left(\frac{A}{b}\right) \left(\frac{b}{A}\right) \\ &= (-1)^{\frac{b-1}{2}} (-1)^{\frac{A-1}{2} \frac{b-1}{2}} \\ &= (-1)^{\frac{b-1}{2} [1 + \frac{A-1}{2}]} \\ &= (-1)^{\frac{b-1}{2} \frac{1+A}{2}} \\ &= (-1)^{\frac{b-1}{2} \frac{a-1}{2}} \end{aligned}$$

So the law of quadratic reciprocity remains valid for the Kronecker symbol when a is negative ($b > 0, a, b$ both odd). \square

Ex. 5.37 Show that if a is negative, then $p \equiv q \pmod{4a}$, $p \nmid a$ implies $(a/p) = (a/q)$.

Proof. Write $a = -A, A > 0$. As $p \equiv q \pmod{4a}$, we know from Prop. 5.3.3. (b) that $(A/p) = (A/q)$.

Moreover,

$$\begin{aligned} \left(\frac{a}{p}\right) &= \left(\frac{-A}{p}\right) = (-1)^{(p-1)/2} \left(\frac{A}{p}\right) \\ \left(\frac{a}{q}\right) &= \left(\frac{-A}{q}\right) = (-1)^{(q-1)/2} \left(\frac{A}{q}\right) \end{aligned}$$

As $p \equiv q \pmod{4a}$, $p = q + 4ak, k \in \mathbb{Z}$, so

$$(-1)^{(p-1)/2} = (-1)^{(q+4ak-1)/2} = (-1)^{(q-1)/2},$$

so $(a/p) = (a/q)$. \square

Ex. 5.38 Let p be an odd prime. Derive the quadratic character of 2 modulo p by verifying the following steps, involving the Jacobi symbol:

$$\left(\frac{2}{p}\right) = \left(\frac{8-p}{p}\right) = \left(\frac{p}{p-8}\right) = \left(\frac{8}{p-8}\right) = \left(\frac{2}{p-8}\right).$$

Generalize the argument to show that

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p-4a}\right), \quad a > 0, p \nmid a.$$

(As in Ex. 5.36, since $8-p$ or $p-8$ is negative, we interpret (a/b) as the Kronecker symbol : see definition in Ex. 5.36.)

Proof. As $(2^2/p) = 1$ and $8-p \equiv 8 \pmod{p}$,

$$\left(\frac{2}{p}\right) = \left(\frac{2^2}{p}\right) \left(\frac{2}{p}\right) = \left(\frac{8}{p}\right) = \left(\frac{8-p}{p}\right).$$

As p and $8-p$ are odd numbers and $p > 0$, from the extension of the law of quadratic reciprocity to $a < 0$ proved in Ex. 5.36, we obtain

$$\left(\frac{8-p}{p}\right) = (-1)^{\frac{7-p}{2} \frac{p-1}{2}} \left(\frac{p}{8-p}\right).$$

Moreover

$$(7-p)(p-1) \equiv (-1-p)(p-1) = 1-p^2 \pmod{8}$$

As $p = 2k+1$ is odd, $p^2 = 4k^2 + 4k + 1 = 8\frac{k(k+1)}{2} + 1 \equiv 1 \pmod{8}$, so $(7-p)(p-1) \equiv 0 \pmod{8}$ and $\frac{7-p}{2} \frac{p-1}{2}$ is even, so

$$\left(\frac{8-p}{p}\right) = \left(\frac{p}{8-p}\right).$$

As $p > 0$, $\left(\frac{p}{-1}\right) = 1$, thus $\left(\frac{p}{8-p}\right) = \left(\frac{p}{-1}\right) \left(\frac{p}{p-8}\right) = \left(\frac{p}{p-8}\right)$ (with the same argument, this is also true for the 3 odd primes such that $8-p > 0$), so

$$\left(\frac{8-p}{p}\right) = \left(\frac{p}{p-8}\right).$$

□

As $p \equiv 8 \pmod{p-8}$, $\left(\frac{p}{p-8}\right) = \left(\frac{8}{p-8}\right)$, and since $8 = 2^2 \times 2$, $\left(\frac{8}{p-8}\right) = \left(\frac{2}{p-8}\right)$. We have proved for all odd primes p that

$$\left(\frac{2}{p}\right) = \left(\frac{8-p}{p}\right) = \left(\frac{p}{p-8}\right) = \left(\frac{8}{p-8}\right) = \left(\frac{2}{p-8}\right).$$

The preceding arguments remain valid if we replace the odd prime p by any odd positive integer. So with an immediate induction, we see that for all $k \in \mathbb{N}$,

$$\left(\frac{2}{p}\right) = \left(\frac{2}{p-8k}\right).$$

So the quadratic character of 2 modulo p depends only of the class of p modulo 8.

If $p \equiv 1 \pmod{8}$, $\left(\frac{2}{p}\right) = \left(\frac{2}{1}\right) = 1$.

If $p \equiv -1 \pmod{8}$, $\left(\frac{2}{p}\right) = \left(\frac{2}{-1}\right) = 1$.

If $p \equiv \pm 3 \pmod{8}$, $\left(\frac{2}{p}\right) = \left(\frac{2}{\pm 3}\right) = -1$.

Generalization : let $a > 0$ and p an odd positive integer such that $p \wedge a = 1$ (not necessarily prime).

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

$(4a-p-1)(p-1) = 4a(p-1) + 1 - p^2 \equiv 0 \pmod{8}$, so

$$\left(\frac{a}{p}\right) = \left(\frac{p}{4a-p}\right).$$

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

$$\left(\frac{p}{4a-p}\right) = \left(\frac{p}{p-4a}\right).$$

Since $p \equiv 4a \pmod{p} - 4a$, and 4 is a square,

$$\left(\frac{p}{p-4a}\right) \equiv \left(\frac{4a}{p-4a}\right) = \left(\frac{a}{p-4a}\right).$$

We have proved

$$\left(\frac{a}{p}\right) = \left(\frac{4a-p}{p}\right) = \left(\frac{p}{p-4a}\right) = \left(\frac{4a}{p-4a}\right) = \left(\frac{a}{p-4a}\right).$$

By induction, for all $k \geq 0$, $\left(\frac{a}{p}\right) = \left(\frac{a}{p-4a}\right)$, so $\left(\frac{a}{p}\right)$ depends only of the class of p modulo $4a$.

Chapter 6

Ex. 6.1 Show that $\sqrt{2} + \sqrt{3}$ is an algebraic integer.

Proof. Let $x = \sqrt{2} + \sqrt{3}$. Then $x^2 = 5 + 2\sqrt{6}$.

$(x^2 - 5)^2 = (2\sqrt{6})^2 = 24$, so $x^4 - 10x^2 + 1 = 0$: x is an algebraic integer. \square

Ex. 6.2 Let α be an algebraic number. Show that there's an integer n such that $n\alpha$ is an algebraic integer.

(0 is a valid answer to this sentence ! More seriously, we search a *positive* integer n .)

Proof. Let α an algebraic number. By definition, there exist $a_0, a_1, \dots, a_n \in \mathbb{Z}, a_n \neq 0$, such that

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_k \alpha^k + \dots + a_0 = 0.$$

(Up to multiply this equation by -1 , we can suppose that $a_n > 0$).

Multiplying by a_n^{n-1} , we obtain

$$a_n^n \alpha^n + a_n^{n-1} a_{n-1} \alpha^{n-1} + \dots + a_n^{n-1} a_k \alpha^k + \dots + a_n^{n-1} a_0 = 0.$$

So

$$(a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + \cdots + a_n^{n-k-1}a_k(a_n\alpha)^k + \cdots + a_n^{n-1}a_0 = 0.$$

Soit $p(x) = x^n + \sum_{k=0}^{n-1} a_n^{n-k-1}a_kx^k$. Then $p(x) \in \mathbb{Z}[x]$, $p(x)$ is monic, and $p(a_n\alpha) = 0$.

So $a_n\alpha$ is an algebraic integer, with $m = a_n \in \mathbb{N}^*$.

Conclusion : if α is an algebraic number, there exists an integer $m > 0$ such that $m\alpha$ is an algebraic integer. \square

Ex. 6.3 If α and β are algebraic integers, prove that any solution to $f(x) = x^2 + \alpha x + \beta = 0$ is an algebraic integer. Generalize this result.

Proof. Let γ a root of $x^2 + \alpha x + \beta$, where α, β verify :

$$\alpha^n + r_1\alpha^{n-1} + \cdots + r_n = 0, \quad r_i \in \mathbb{Z},$$

$$\beta^m + s_1\beta^{m-1} + \cdots + s_m = 0, \quad s_j \in \mathbb{Z}.$$

Let V the set of linear combinations with integer coefficients of

$$\alpha^i\beta^j\gamma^k, 0 \leq i < n, 0 \leq j < m, 0 \leq k < 2.$$

Then V is a finitely generated \mathbb{Z} -module.

Moreover, for all $\delta \in V, \gamma\delta \in V$. Indeed, every $\delta \in V$ is a linear combination with coefficients in \mathbb{Z} of $\alpha^i\beta^j, \alpha^i\beta^j\gamma$, and

$$\gamma(\alpha^i\beta^j) = \alpha^i\beta^j\gamma \in V$$

$$\gamma(\alpha^i\beta^j\gamma) = \alpha^i\beta^j\gamma^2 = \alpha^i\beta^j(-\alpha\gamma - \beta) = -\alpha^{i+1}\beta^j\gamma - \alpha^i\beta^{j+1} \in V.$$

(if $i+1 = n$, we replace $\alpha^{i+1} = \alpha^n$ by $-\sum_{k=1}^{n-1} r_k\alpha^{n-k}$, and a similar replacement if $j+1 = m$.)

As for each $x \in V$, where V is a finitely generated \mathbb{Z} -module, $x\gamma \in V$, so γ is an algebraic integer (Proposition 6.1.4).

More generally, if $\gamma^n + \alpha_1\gamma^{n-1} + \cdots + \alpha_n = 0$, where the α_i are algebraic integers, then x is an algebraic integer. \square

Ex. 6.4 A polynomial $f(x) \in \mathbb{Z}[x]$ is said to be primitive if the greatest common divisor of its coefficients is 1. Prove that product of primitive polynomials is also primitive.

Solution 1

Proof. Let $p(x) = \sum_{i=0}^n a_ix^i, q(x) = \sum_{j=0}^m b_jx^j$ two primitive polynomials, and p a prime number. There exist a coefficient of $p(x)$ (and of $q(x)$) not divisible by p . Let

$$i_0 = \min\{i \in [0, n] \mid a_i \not\equiv 0 \pmod{p}\}$$

$$j_0 = \min\{j \in [0, m] \mid b_j \not\equiv 0 \pmod{p}\}$$

Let $p(x)q(x) = \sum_{k=0}^{n+m} c_kx^k$. Then $c_k = \sum_{i+j=k} a_ib_j, k = 0, \dots, n+m$. Then

$$c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_ib_j.$$

- If $i < i_0$, then $a_i \equiv 0 \pmod{p}$.
- If $i > i_0$, then $j < j_0$ and $b_j \equiv 0 \pmod{p}$.

In the two cases $a_i b_j \equiv 0 \pmod{p}$, so $c_{i_0+j_0} \equiv a_{i_0} b_{j_0} \pmod{p}$, so $c_{j_0} \not\equiv 0 \pmod{p}$: as it's true for all primes p , the polynomial $p(x)q(x)$ is primitive. \square

Solution 2

Proof. Let

$$\varphi : \begin{cases} \mathbb{Z}[x] & \rightarrow \mathbb{F}_p[x] \\ p(x) = a_0 + \cdots + a_n x^n & \mapsto \bar{p}(x) = \bar{a}_0 + \cdots + \bar{a}_n x^n, \end{cases}$$

where \bar{a}_i is the class of a_i in \mathbb{F}_p . φ is a ring homomorphism.

As $\mathbb{F}_p[x]$ is an integrity domain, if $p(x), q(x)$ are both primitive,

$$\overline{p(x)} \neq 0, \overline{q(x)} \neq 0 \Rightarrow \overline{p(x)q(x)} = \overline{p(x)} \overline{q(x)} \neq 0.$$

As $\overline{p(x)q(x)} \neq 0$ in all fields \mathbb{F}_p , $p(x)q(x)$ is a primitive polynomial. \square

Ex. 6.5 Let α be an algebraic integer and $f(x) \in \mathbb{Q}[x]$ be the monic polynomial of least degree such that $f(\alpha) = 0$. Use Exercise 6.4 to show that $f(x) \in \mathbb{Z}[x]$.

Proof. As α is an algebraic integer, there exists a monic polynomial $h(x) \in \mathbb{Z}[x]$ such that $h(\alpha) = 0$. As $f(x) \in \mathbb{Q}[x]$ is the minimal polynomial of α , and $h(\alpha) = 0$, $f(x)$ divides $h(x)$ in $\mathbb{Q}[x]$.

(quick reminder : $h(x) = q(x)f(x) + r(x)$, $q(x), r(x) \in \mathbb{Q}[x]$, $\deg(r(x)) < \deg(f(x))$ or $r(x) = 0$. As $r(\alpha) = 0$ and $f(x) \in \mathbb{Q}[x]$ is the monic polynomial of least degree such that $f(\alpha) = 0$, $r = 0$ so $f(x) \mid h(x)$).

So there exists $g(x) \in \mathbb{Q}[x]$ such that $h(x) = f(x)g(x)$. As $h(x), f(x)$ are both monic, $g(x)$ is also monic.

Let $d \in \mathbb{Z}, d \neq 0$ such that $df(x) = \sum_{i=0}^m a_i x^i \in \mathbb{Z}[x]$, and $c = a_1 \wedge a_2 \wedge \cdots \wedge a_m$, $a_i = cb_i$, with $b_1 \wedge b_2 \wedge \cdots \wedge b_m = 1$, so $f(x) = \frac{c}{d} f_1(x)$, with f_1 is primitive. Similarly $g(x) = \frac{s}{t} g_1(x)$, $s, t \in \mathbb{Z}$, $g_1(x)$ primitive.

So $h(x) = \frac{cs}{dt} f_1(x)f_2(x) = \frac{u}{v} f_1(x)f_2(x)$, where $u \wedge v = 1$. The polynomial $f_1(x)f_2(x) = \sum_{k=0}^r c_k x^k$ is primitive (Ex. 6.4). As $vh(x)(x) = uf_1(x)f_2(x)$, $v \mid uc_k$, and $u \wedge v = 1$, thus $v \mid c_k, k = 0, 1, \dots, r$. As $c_1 \wedge \cdots \wedge c_r = 1$, $v \mid 1$, so $v = \pm 1$. $h(x) = uf_1(x)f_2(x)$ is monic, thus $u = 1$, and f_1, f_2 are monic. From $f(x) = \frac{c}{d} f_1(x)$ we deduce $\frac{c}{d} = 1$ and $f(x) = f_1(x) \in \mathbb{Z}[x]$.

Conclusion : if $f(x)$ is the minimal polynomial of an algebraic integer α , $f \in \mathbb{Z}[x]$. \square

Ex. 6.6 Let $x^2 + mx + n \in \mathbb{Z}[x]$ be irreducible, and α be a root. Show that $\mathbb{Q}[\alpha] = \{r + s\alpha : r, s \in \mathbb{Q}\}$ is a ring (in fact, it is a field). Let $m^2 - 4n = D_0^2 D$, where D is square-free. Show that $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{D}]$.

Proof. By definition, for all $z \in \mathbb{C}, z \in \mathbb{Q}[\alpha] \iff \exists P \in \mathbb{Q}[x], z = P(\alpha)$.

The Euclidean division gives $P = Q_1(x^2 + mx + n) + R$, $Q_1, R \in \mathbb{Q}[x]$, $\deg(R) < 2$, so $R = rx + s$, $r, s \in \mathbb{Q}$. So $z = Q_1(\alpha)(\alpha^2 + m\alpha + n) + r\alpha + s = r\alpha + s$:

$$\mathbb{Q}[\alpha] = \{z \in \mathbb{C} \mid \exists r \in \mathbb{Q}, \exists s \in \mathbb{Q}, z = r + s\alpha\}.$$

• $\mathbb{Q}[\alpha] \subset \mathbb{C}$, where $(\mathbb{C}, +, \times)$ is a field. $1 \in \mathbb{Q}[\alpha]$ ($1 = P_0(\alpha)$, where P_0 is the constant polynomial 1).

• Let $\beta, \gamma \in \mathbb{Q}[\alpha] : \beta = P(\alpha), \gamma = Q(\alpha)$, where P, Q are in $\mathbb{Q}[x]$. Then $\alpha - \beta = P(\alpha) - Q(\alpha) = R(\alpha)$, where $R = P - Q \in \mathbb{Q}[x]$, and $\alpha\beta = P(\alpha)Q(\alpha) = S(\alpha)$, where $S = PQ \in \mathbb{Q}[x]$. So $\alpha - \beta \in \mathbb{Q}[\alpha], \alpha\beta \in \mathbb{Q}[\alpha]$. So $\mathbb{Q}[\alpha]$ is a subring of $(\mathbb{C}, +, \times)$.

• Let $\beta = P(\alpha) \in \mathbb{Q}[\alpha], P \in \mathbb{Q}[x]$ and $\beta \neq 0$. As $\beta \neq 0, Q = x^2 + mx + n \nmid P$.

Let $D \in \mathbb{Q}[x]$ such that $D \mid P, D \mid Q$. As Q is irreducible by hypothesis, $D = \lambda$ or $D = \lambda Q, \lambda \in \mathbb{C}^*$ (D is an associate of 1 or Q). If $D = \lambda Q$, then $Q \mid D$, and $D \mid P$, so $Q \mid P$. Since $Q(\alpha) = 0$, this implies $\beta = P(\alpha) = 0$, in contradiction with the definition of β . So $D = \lambda \mid 1$. Therefore $P \wedge Q = 1$.

From Bézout's theorem, there exist polynomials $U, V \in \mathbb{Q}[x]$ such that $UP + VQ = 1$. As $\mathbb{Q}(\alpha) = 0, U(\alpha)P(\alpha) = 1$ and $\gamma = U(\alpha) \in \mathbb{Q}[\alpha]$ is such that $\gamma\beta = 1$. Therefore $\mathbb{Q}[\alpha]$ is a subfield of $(\mathbb{C}, +, \times)$ (and $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$).

As $x^2 + mx + n$ is irreducible, $\Delta = m^2 - 4n \neq 0$ (if not, $x^2 + mx + n = (x + m/2)^2 - (m^2 - 4n)/4 = (x + m/2)^2$ is not irreducible). So $\Delta \in \mathbb{Z} \setminus \{0\}$ can be written $\Delta = m^2 - 4n = D_0^2 D$, where D is square-free (positive or negative), $D \neq 0, D_0 \neq 0$.

$\alpha = -\frac{m}{2} + \varepsilon \frac{\sqrt{\Delta}}{2}, \varepsilon = \pm 1$, so $\alpha = -\frac{m}{2} + \varepsilon D_0 \frac{\sqrt{D}}{2}$, thus $\alpha \in \mathbb{Q}[\sqrt{D}]$ and $\mathbb{Q}[\alpha] \subset \mathbb{Q}[\sqrt{D}]$.

As $D_0 \neq 0, \sqrt{D} = \varepsilon \frac{2\alpha + m}{D_0} \in \mathbb{Q}[\alpha]$, so $\mathbb{Q}[\sqrt{D}] \subset \mathbb{Q}[\alpha]$:

$$\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{D}].$$

□

Ex. 6.7 (continuation) If $D \equiv 2, 3 \pmod{4}$, show that all the algebraic integers in $\mathbb{Q}[\sqrt{D}]$ have the form $a + b\sqrt{D}$, where $a, b \in \mathbb{Z}$. If $D \equiv 1 \pmod{4}$, show that all the algebraic integers in $\mathbb{Q}[\sqrt{D}]$ have the form $a + b((-1 + \sqrt{D})/2)$, where $a, b \in \mathbb{Z}$.

Proof. (We write $\overline{\mathbb{Z}}$ the ring of algebraic integers in \mathbb{C} , and \mathcal{O}_K (or \mathbb{Z}_K) the ring of algebraic integers in the field K .)

If $D = 1, \mathbb{Q}[\sqrt{D}] = \mathbb{Q}$. If $D \neq 1$, as D is square-free, D is not a square, so \sqrt{D} is irrational.

Let $\gamma = r + s\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$ ($r, s \in \mathbb{Q}$) an algebraic integer of $\mathbb{Q}[\sqrt{D}]$ ($D \in \mathbb{Z}, D$ square-free). $(\gamma - r)^2 = s^2 D$, so $\gamma^2 - 2r\gamma + r^2 - Ds^2 = 0$. γ is a root of

$$p(x) = x^2 - 2rx + r^2 - Ds^2.$$

If $s = 0$, then the minimal polynomial of γ is $x - r$. As $r = \gamma$ is an algebraic integer and $r \in \mathbb{Q}$, then $r \in \mathbb{Z}$. In this case $r \in \mathbb{Z}$ and $s = 0$.

If $s \neq 0, \gamma \notin \mathbb{Q}$, so no polynomial of degree $d \leq 1$ has the root γ . Thus the minimal polynomial of γ is $p(x)$. From Exercise 6.5, $p(x) \in \mathbb{Z}[x]$, so (in the two cases $s = 0, s \neq 0$)

$$2r \in \mathbb{Z}, r^2 - Ds^2 \in \mathbb{Z}.$$

Conversely, if $2r \in \mathbb{Z}, r^2 - Ds^2 \in \mathbb{Z}$, then $p(x) \in \mathbb{Z}[x]$ and $p(\gamma) = 0$, thus γ is an algebraic integer.

If $r, s \in \mathbb{Q}, D \neq 1$ square-free,

$$r + s\sqrt{D} \in \overline{\mathbb{Z}} \iff 2r \in \mathbb{Z}, r^2 - Ds^2 \in \mathbb{Z}.$$

Let $\gamma = r + s\sqrt{D} \in \overline{\mathbb{Z}}$. We can write

$$r = \frac{a}{d}, s = \frac{b}{d}, \quad a, b, d \in \mathbb{Z}, d \geq 1, d \wedge a \wedge b = 1.$$

Then

$$n = \frac{2a}{d} \in \mathbb{Z}, \quad m = \frac{a^2 - Db^2}{d^2} \in \mathbb{Z}.$$

As D is square-free, $D \not\equiv 0 \pmod{4}$.

- Case 1 : $D \equiv 2, 3 \pmod{4}$.

$$n^2 - 4m = \frac{4Db^2}{d^2}, \text{ so } d \mid 2a, d^2 \mid 4Db^2.$$

If $2 \mid d$, $4 \mid a^2 - Db^2$, $a^2 \equiv Db^2 \pmod{4}$. As $d \wedge a \wedge b = 1$, and $2 \mid d$, a or b is odd, and $a^2 \equiv Db^2 \pmod{4}$, $D \not\equiv 0 \pmod{4}$, implies that a and b are both odd. Then $a^2 \equiv b^2 \equiv 1 \pmod{4}$, so $D \equiv 1 \pmod{4}$: this is in contradiction with the hypothesis $D \equiv 2, 3 \pmod{4}$. So d is an odd number.

Consequently, $d \mid a, d^2 \mid Dq^2$. If $p \in \mathbb{N}$ is a prime factor of d , $p \mid d, p \mid a$, and $d \wedge a \wedge b = 1$, so $p \nmid b$, and since $p^2 \mid Db^2$, $p^2 \mid D$, in contradiction with D square-free. So $d \geq 1$ has no prime factor : $d = 1$ and $r = a, s = b \in \mathbb{Z}$. Conversely, any $\gamma = a + b\sqrt{D}, a, b \in \mathbb{Z}$ is an algebraic integer, so

$$\mathcal{O}_{\mathbb{Q}[\sqrt{D}]} = \overline{\mathbb{Z}} \cap \mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}.$$

- Case 2 : $D \equiv 1 \pmod{4}$.

Then $r = \frac{n}{2}, n \in \mathbb{Z}$. Write $s = \frac{u}{v}, u \wedge v = 1, v \geq 1$.

$m = r^2 - Ds^2 = \frac{n^2}{4} - D\frac{u^2}{v^2} \in \mathbb{Z}$, $4D\frac{u^2}{v^2} = n^2 - 4m \in \mathbb{Z}$, so $v^2 \mid 4Du^2$. Since $u \wedge v = 1, u^2 \wedge v^2 = 1$, so $v^2 \mid 4D$. As D is square-free, v has no odd prime factor, so $v = 2^k$. Since D is odd, $k \leq 1$ and $v = 1$ or $v = 2$. So r, s are both half-integers: $r = n/2, s = n'/2, n, n' \in \mathbb{Z}$.

$4m = n^2 - Dn'^2$, thus $n^2 \equiv n'^2 \pmod{4}$, so n, n' have the same parity. Let $a = \frac{n+n'}{2} \in \mathbb{Z}, b = n' \in \mathbb{Z}$. Then $n = 2a - b, n' = b$ and $\gamma = \frac{n}{2} + \frac{n'}{2}\sqrt{D} = a - \frac{b}{2} + \frac{b}{2}\sqrt{D} = a + b\left(\frac{-1+\sqrt{D}}{2}\right)$.

Conversely, $\frac{-1+\sqrt{D}}{2}$ is a root of $x^2 + x + \frac{1-D}{4} \in \mathbb{Z}[x]$, so every $a + b\left(\frac{-1+\sqrt{D}}{2}\right)$ is an algebraic integer.

$$\mathcal{O}_{\mathbb{Q}[\sqrt{D}]} = \overline{\mathbb{Z}} \cap \mathbb{Q}[\sqrt{D}] = \left\{a + b\left(\frac{-1+\sqrt{D}}{2}\right) \mid a, b \in \mathbb{Z}\right\}.$$

□

Ex. 6.8 Let $\omega = e^{2\pi i/3}$, ω satisfies $x^3 - 1 = 0$. Show that $(2\omega + 1)^2 = -3$, and use this to determine $(-3/p)$ by the method of section 2.

Proof. As $\omega^2 + \omega + 1 = 0, (2\omega + 1)^2 = 4\omega^2 + 4\omega + 1 = -4 + 1 = -3$. Let $\alpha = 2\omega + 1$, so $\alpha^2 = -3$

$$\left(\frac{-3}{p}\right) \equiv (-3)^{(p-1)/2} \pmod{p}$$

$$\equiv \alpha^{p-1} \pmod{p}$$

$$\alpha^p = \left(\frac{-3}{p}\right)\alpha.$$

From Prop. 6.1.6,

$$\begin{aligned}\alpha^p &= (2\omega + 1)^p \\ &\equiv 2^p \omega^p + 1 \pmod{p} \\ &\equiv 2\omega^p + 1 \pmod{p}\end{aligned}$$

- If $p \equiv 0 \pmod{3}$, $\left(\frac{-3}{p}\right) = 0$.
- If $p \equiv 1 \pmod{3}$, $\omega^p = \omega$, so $\alpha^p \equiv \alpha \pmod{p}$.
 $\left(\frac{-3}{p}\right)\alpha \equiv \alpha \pmod{p}$, thus $\left(\frac{-3}{p}\right)\alpha^2 \equiv \alpha^2 \pmod{p}$, $\left(\frac{-3}{p}\right)3 \equiv 3 \pmod{p}$. As $p \wedge 3 = 1$,
 $\left(\frac{-3}{p}\right) \equiv 1 \pmod{p}$. Since $\left(\frac{-3}{p}\right) = \pm 1$, $\left(\frac{-3}{p}\right) = 1$.
- If $p \equiv -1 \pmod{3}$,

$$\begin{aligned}\alpha^p &\equiv 2\omega^p + 1 \pmod{p} \\ &\equiv 2\omega^2 + 1 = 2(-1 - \omega) + 1 = -2\omega - 1 = -\alpha \pmod{p}.\end{aligned}$$

$\left(\frac{-3}{p}\right)\alpha \equiv -\alpha \pmod{p}$, thus $\left(\frac{-3}{p}\right)\alpha^2 \equiv -\alpha^2 \pmod{p}$, $\left(\frac{-3}{p}\right)3 \equiv -3 \pmod{p}$. As
 $p \wedge 3 = 1$, $\left(\frac{-3}{p}\right) \equiv -1 \pmod{p}$. Since $\left(\frac{-3}{p}\right) = \pm 1$, $\left(\frac{-3}{p}\right) = -1$.

Conclusion :

$$\begin{aligned}p \equiv 0[3] &\iff \left(\frac{-3}{p}\right) = 0 \\ p \equiv 1[3] &\iff \left(\frac{-3}{p}\right) = 1 \\ p \equiv -1[3] &\iff \left(\frac{-3}{p}\right) = -1\end{aligned}$$

In other words, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$.

Note : $\alpha = 2\omega + 1 = \omega - \omega^2 = g$, the quadratic Gauss sum for $p = 3$. □

Ex. 6.9 Verify Proposition 6.3.2 explicitly for $p = 3, 5$, i.e., write out the Gauss sum longhand and square.

Proof. • $p=3$. Let $\omega = e^{2i\pi/3}$. Let $g = \sum_{t=0}^2 (t/3)\omega^t$ the quadratic Gauss sum. Then
 $g = \omega - \omega^2$.

As $1 + \omega + \omega^2 = 0$, $g^2 = (\omega - \omega^2)^2 = \omega^2 - 2\omega^3 + \omega^4 = \omega^2 - 2 + \omega = -3$:

$$g^2 = -3.$$

- $p=5$. Let $\zeta = e^{2i\pi/5}$.
 $g = \sum_{t=0}^4 (t/5)\zeta^t = \zeta - \zeta^2 - \zeta^3 + \zeta^4$.
Then $g = \alpha - \beta$, where $\alpha = \zeta + \zeta^4, \beta = \zeta^2 + \zeta^3$.
 $\alpha + \beta = \zeta + \zeta^4 + \zeta^2 + \zeta^3 = -1$.
 $\alpha\beta = \zeta^3 + \zeta^4 + \zeta^6 + \zeta^7 = \zeta^3 + \zeta^4 + \zeta + \zeta^2 = -1$

So α, β are the two roots of $x^2 + x - 1$.

$$\begin{aligned}
 g^2 &= (\alpha - \beta)^2 \\
 &= \alpha^2 + \beta^2 - 2\alpha\beta \\
 &= (\alpha + \beta)^2 - 4\alpha\beta \\
 &= (-1)^2 - 4(-1) \\
 &= 5.
 \end{aligned}$$

Note : here we know explicitly g :

if $p = 3$, $g = \omega - \omega^2 = i\sqrt{3}$.

If $p = 5$, $g = \alpha - \beta = (-1 + \sqrt{5})/2 - (-1 - \sqrt{5})/2 = \sqrt{5}$.

□

Ex. 6.10 What is $\sum_{a=1}^{p-1} g_a$?

Proof. From Prop. 6.3.1 and Lemma 2,

$$\sum_{a=1}^{p-1} g_a = g_1 \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

□

Ex. 6.11 By evaluating $\sum_t (1 + (t/p))\zeta^t$ in two ways, prove that $g = \sum_t \zeta^{t^2}$.

Proof. For $a \in \mathbb{F}_p$, Write $N[x^2 = a]$ the number of solutions of the equation $x^2 = a$ in \mathbb{F}_p . We know from Ex. 5.2 that $N[x^2 = a] = 1 + (a/p)$. So

$$\begin{aligned}
 \sum_{t=0}^{p-1} \zeta^{t^2} &= \sum_{\bar{t} \in \mathbb{F}_p} \zeta^{t^2} \\
 &= \sum_{\bar{t} \in \mathbb{F}_p} N[x^2 = t] \zeta^t \\
 &= \sum_{\bar{t} \in \mathbb{F}_p} \left(1 + \left(\frac{t}{p}\right)\right) \zeta^t \\
 &= \sum_{\bar{t} \in \mathbb{F}_p} \zeta^t + \sum_{\bar{t} \in \mathbb{F}_p} \left(\frac{t}{p}\right) \zeta^t \\
 &= \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^t \\
 &= g
 \end{aligned}$$

□

Ex. 6.12 Write $\psi_a(t) = \zeta^{at}$. Show that

$$(a) \quad \overline{\psi_a(t)} = \psi_a(-t) = \psi_{-a}(t)$$

$$(b) \quad (1/p) \sum_a \psi_a(t-s) = \delta(t, s)$$

Proof. (a) Let $a \in \mathbb{Z}$. As $\bar{\zeta} = \zeta^{-1}$,

$$\begin{aligned} \overline{\psi_a(t)} &= \overline{\zeta^{at}} = \zeta^{-at} \\ &= \zeta^{a(-t)} = \zeta^{(-a)t} \\ &= \psi_a(-t) = \psi_{-a}(t) \end{aligned}$$

$$\overline{\psi_a(t)} = \psi_a(-t) = \psi_{-a}(t)$$

(b) From Corollary of Lemma 1 :

$$\begin{aligned} \frac{1}{p} \sum_{a=0}^{p-1} \psi_a(t-s) &= \frac{1}{p} \sum_{a=0}^{p-1} \zeta^{a(t-s)} = \delta(t, s) \\ \frac{1}{p} \sum_a \psi_a(t-s) &= \delta(t, s). \end{aligned}$$

□

Ex. 6.13 Let f be a function from \mathbb{Z} to the complex numbers. Suppose that p is a prime and that $f(n+p) = f(n)$ for all $n \in \mathbb{Z}$. Let $\hat{f}(a) = p^{-1} \sum_t f(t) \psi_{-a}(t)$. Prove that $f(t) = \sum_a \hat{f}(a) \psi_a(t)$. This result is directly analogous to a result in the theory of Fourier series.

Proof. Let $\hat{f}(a) = p^{-1} \sum_t f(t) \psi_{-a}(t)$. Then

$$\begin{aligned} \sum_{a=0}^{p-1} \hat{f}(a) \psi_a(t) &= \sum_{a=0}^{p-1} p^{-1} \sum_{s=0}^{p-1} f(s) \psi_{-a}(s) \psi_a(t) \\ &= p^{-1} \sum_{s=0}^{p-1} f(s) \sum_{a=0}^{p-1} \psi_{-a}(s) \psi_a(t) \\ &= p^{-1} \sum_{s=0}^{p-1} f(s) \sum_{a=0}^{p-1} \psi_a(t-s) \\ &= \sum_{s=0}^{p-1} f(s) \delta(s, t) \\ &= f(t) \end{aligned}$$

□

Ex. 6.14 In Ex. 13 take f to be the Legendre symbol and show that $\hat{f}(a) = p^{-1} g_{-a}$.

Proof. Here $f(a) = \left(\frac{a}{p}\right)$. Then $\hat{f}(a) = p^{-1} \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{-at} = p^{-1} g_{-a}$. □

Ex. 6.15 Show that

$$\left| \sum_{t=n}^m \binom{t}{p} \right| < \sqrt{p} \log p.$$

The inequality holds for the sum over any range.

Lemma. If $0 \leq x \leq \frac{\pi}{2}$, $\sin x \geq \frac{2}{\pi}x$.

Proof. As $-\sin$ is a convex function on $[0, \pi/2]$, the graph of \sin is above any chord, and the chord between the points $(0, 0)$ and $(\pi/2, 1)$ has equation $y = (2/\pi)x$, we conclude that $\sin x \geq \frac{2}{\pi}x$ for $0 \leq x \leq \pi/2$. \square

Proof. Let $S = \sum_{t=n}^m \binom{t}{p} g$ with $n \leq m$. Then $|S| = \sqrt{p} \left| \sum_{t=n}^m \binom{t}{p} \right|$. As $(t/p)g = g_t$,

$$\begin{aligned} S &= \sum_{t=m}^n g_t \\ &= \sum_{t=m}^n \sum_{s=0}^{p-1} \binom{s}{p} \zeta^{ts} \\ &= \sum_{s=0}^{p-1} \binom{s}{p} \zeta^{ms} \sum_{t=m}^n \zeta^{(t-m)s} \\ &= \sum_{s=0}^{p-1} \binom{s}{p} \zeta^{ms} \sum_{u=0}^{n-m} \zeta^{us} \quad (u = t - m) \\ &= \sum_{s=1}^{p-1} \binom{s}{p} \zeta^{ms} \frac{\zeta^{(n-m+1)s} - 1}{\zeta^s - 1} \end{aligned}$$

(since for $s = 0$, the sum $\sum_{u=0}^{n-m} \zeta^{us} = n - m + 1$ and $\binom{s}{p} = 0$). So

$$\begin{aligned} S &= \sum_{s=1}^{p-1} \binom{s}{p} \frac{\zeta^{(n+1)s} - \zeta^{ms}}{\zeta^s - 1} \\ &= \sum_{s=1}^{p-1} \binom{s}{p} \frac{\zeta^{\frac{n+m+1}{2}s}}{\zeta^{\frac{s}{2}}} \frac{\zeta^{\frac{n-m+1}{2}s} - \zeta^{\frac{-n+m-1}{2}s}}{\zeta^{\frac{s}{2}} - \zeta^{\frac{-s}{2}}} \\ &= \sum_{s=1}^{p-1} \binom{s}{p} \zeta^{\frac{n+m}{2}s} \frac{\sin\left((n-m+1)s\frac{\pi}{p}\right)}{\sin\left(s\frac{\pi}{p}\right)} \end{aligned}$$

As $\sin(x) \geq \frac{2}{\pi}x$ for $x \in [0, \frac{\pi}{2}]$, for all s , $1 \leq s < \frac{p}{2}$, $0 \leq \frac{s\pi}{p} \leq \frac{\pi}{2}$, so

$$\left| \frac{\sin\left((n-m+1)s\frac{\pi}{p}\right)}{\sin\left(s\frac{\pi}{p}\right)} \right| \leq \frac{1}{\frac{2}{\pi}\left(s\frac{\pi}{p}\right)} = \frac{p}{2s} \quad (s = 1, 2, \dots, (p-1)/2).$$

Since $\binom{s}{p} \zeta^{ts}$ depends only of the class of s , we can replace in the preceding calculation the values $s = 1, 2, \dots, p-1$ by $s = -(p-1)/2, \dots, -1, 1, \dots, (p-1)/2$, so

$$S = \sum_{s=1}^{(p-1)/2} \binom{s}{p} \zeta^{\frac{n+m}{2}s} \frac{\sin\left((n-m+1)s\frac{\pi}{p}\right)}{\sin\left(s\frac{\pi}{p}\right)} + \sum_{s=-(p-1)/2}^{-1} \binom{s}{p} \zeta^{\frac{n+m}{2}s} \frac{\sin\left((n-m+1)s\frac{\pi}{p}\right)}{\sin\left(s\frac{\pi}{p}\right)}.$$

As \sin is an odd function,

$$S = \sum_{s=1}^{(p-1)/2} \left(\frac{s}{p}\right) \zeta^{\frac{n+m}{2}s} \frac{\sin\left((n-m+1)s\frac{\pi}{p}\right)}{\sin\left(s\frac{\pi}{p}\right)} + \sum_{s=1}^{(p-1)/2} \left(\frac{-s}{p}\right) \zeta^{-\frac{n+m}{2}s} \frac{\sin\left((n-m+1)s\frac{\pi}{p}\right)}{\sin\left(s\frac{\pi}{p}\right)}.$$

Thus

$$|S| \leq 2 \sum_{s=1}^{(p-1)/2} \frac{p}{2s} = p \sum_{s=1}^{(p-1)/2} \frac{1}{s}.$$

As $S = \sum_{t=n}^m \left(\frac{t}{p}\right)g$ and $|g| = \sqrt{p}$,

$$\left| \sum_{t=n}^m \left(\frac{t}{p}\right) \right| \leq \sqrt{p} \sum_{s=1}^{(p-1)/2} \frac{1}{s}.$$

It remains to do a sufficient estimation of the harmonic sum. We prove by induction that for all $n \geq 1$,

$$1 + \frac{1}{2} + \cdots + \frac{1}{n} \leq \log(2n+1).$$

As $1 \leq \log(3)$, this proposition is true for $n = 1$. Suppose that it is true for $n - 1$:

$$1 + \frac{1}{2} + \cdots + \frac{1}{n-1} \leq \log(2n-1).$$

Then

$$1 + \frac{1}{2} + \cdots + \frac{1}{n} \leq \frac{1}{n} + \log(2n-1).$$

If we prove that $\frac{1}{n} + \log(2n-1) \leq \log(2n+1)$, the induction is done.

Let $u(x) = \log(2x+1) - \log(2x-1) - \frac{1}{x}$, $x > \frac{1}{2}$.

$$\begin{aligned} u'(x) &= \frac{2}{2x+1} - \frac{2}{2x-1} + \frac{1}{x^2} \\ &= \frac{-4}{4x^2-1} + \frac{1}{x^2} \\ &= \frac{-1}{(4x^2-1)x^2} < 0 \end{aligned}$$

As $u(x) = \log\left(\frac{2x+1}{2x-1}\right) - \frac{1}{x}$, $\lim_{x \rightarrow +\infty} u(x) = 0$. Moreover u is a decreasing function, so for all $x > 1/2$, $u(x) > 0$, and for all $n \in \mathbb{N}$, $n \geq 1$,

$$\frac{1}{n} + \log(2n-1) \leq \log(2n+1).$$

We have proved by induction that for all $n \geq 1$,

$$1 + \frac{1}{2} + \cdots + \frac{1}{n} \leq \log(2n+1).$$

If $n = (p-1)/2$, where p is an odd prime ($p \geq 3$),

$$\sum_{s=1}^{(p-1)/2} \frac{1}{s} \leq \log p.$$

Conclusion :

$$\left| \sum_{t=n}^m \left(\frac{t}{p}\right) \right| < \sqrt{p} \log p.$$

□

Ex. 6.16 Let α be an algebraic number with minimal polynomial $f(x)$. Show that $f(x)$ does not have repeated roots in \mathbb{C} .

Proof. Let γ a repeated root of $f(x)$. Then $f(\gamma) = f'(\gamma) = 0$, so $x - \gamma$ is a common factor of f and f' . Thus $f \wedge f' \neq 1$ ($\deg(f \wedge f') \geq 1$). Since $f \wedge f' \mid f$ and f is irreducible (with $f, f \wedge f'$ monic), we conclude $f \wedge f' = f$, so $f \mid f'$. In \mathbb{C} , this is impossible since $\deg(f) \geq 1$, so $f' \neq 0$, and $\deg(f') < \deg(f)$. $f(x)$ does not have repeated roots in \mathbb{C} . \square

Ex. 6.17 Show that the minimal polynomial for $\sqrt[3]{2}$ is $x^3 - 2$.

Proof. Let $f(x) = x^3 - 2$. Then $f(\sqrt[3]{2}) = 0$. If $f(x)$ was not irreducible, then $f(x) = u(x)v(x)$, with $1 \leq \deg(u) \leq \deg(v) \leq 2$, $\deg(u) + \deg(v) = \deg(f) = 3$, so $\deg(u) = 1$, $\deg(v) = 2$.

Then $f(x) = (ax + b)(cx^2 + dx + e)$, $a, b, c, d, e \in \mathbb{Q}$. Let $w = -b/a$. Then $f(w) = w^3 - 2 = 0$ and $w \in \mathbb{Q}$, so there exist $p, q \in \mathbb{Z}$, such that $w = p/q$, $p \wedge q = 1$.

Thus $p^3 = 2q^3$, so p^3 is even, therefore p is even : $p = 2p', p' \in \mathbb{Z}$.

$8p'^3 = 2q^3$, $4p'^3 = q^3$, so q^3 is even, which implies that q is even. Then $2 \mid p \wedge q = 1$: this is a contradiction.

So $f(\sqrt[3]{2}) = 0$, and f is monic, irreducible : f is the minimal polynomial of $\sqrt[3]{2}$ on \mathbb{Q} . \square

Ex. 6.18 Show that there exist algebraic numbers of arbitrarily high degree.

Proof. As $1 + x + \dots + x^{p-1}$ is irreducible on $\mathbb{Q}[x]$ (Prop. 6.4.1), the numbers $\zeta_p = e^{2i\pi/p}$, with p prime number, are algebraic numbers of arbitrary large degree. \square

Ex. 6.19 Find the conjugates of $\cos(2\pi/5)$.

Proof. Let $\gamma = \cos(2\pi/5)$, $\zeta = e^{2i\pi/5}$ and $\alpha = \zeta + \zeta^4, \beta = \zeta^2 + \zeta^3$.

Then $\gamma = \frac{\zeta + \zeta^{-1}}{2} = \frac{\zeta + \zeta^4}{2} = \frac{\alpha}{2}$.

$\alpha + \beta = \zeta + \zeta^4 + \zeta^2 + \zeta^3 = -1$.

$\alpha\beta = \zeta^3 + \zeta^4 + \zeta^6 + \zeta^7 = \zeta^3 + \zeta^4 + \zeta + \zeta^2 = -1$

So α, β are the two roots of $x^2 + x - 1$:

$\alpha^2 + \alpha - 1 = 0$, so $4(\alpha/2)^2 + 2(\alpha/2) - 1 = 0$: $\gamma = \alpha/2$ is a root of

$$f(x) = 4x^2 + 2x - 1.$$

As $\Delta = 4 \times 5$, the two roots of f are irrational. $\deg(f) = 2$ and f has no root in \mathbb{Q} , so $f(x)$ is irreducible in $\mathbb{Q}[x]$. Therefore the minimal polynomial of $\gamma = \cos(2\pi/5)$ is $f(x) = 4x^2 + 2x - 1$. The other root of f is $\beta/2 = (\zeta^2 + \zeta^3)/2 = \cos(4\pi/5)$.

Conclusion : the conjugates of $\gamma = \cos(2\pi/5)$ are $\gamma = \cos(2\pi/5)$ and $\cos(4\pi/5)$. \square

Ex. 6.20 Let F be a subfield of \mathbb{C} which is a finite-dimensional vector space over \mathbb{Q} of degree n . Show that every element of F is algebraic of degree at most n .

Proof. Let $\alpha \in F$, with $\dim_{\mathbb{Q}} F = n$. Any subset of $n + 1$ vectors in F is linearly dependent, so $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ is linearly dependent.

Thus there exists $(a_0, \dots, a_n) \in \mathbb{Q}^{n+1}$, $(a_0, \dots, a_n) \neq (0, 0, \dots, 0)$ such that $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$.

Let $f(x) = a_0 + a_1x + \dots + a_nx^n$. Then $f(x) \in \mathbb{Q}[x]$, $f(x) \neq 0$ and $f(\alpha) = 0$, $\deg(f(x)) \leq n$. So every element of F is algebraic of degree at most n . \square

Ex. 6.21 Let $f(x) = \sum_{n=0}^{\infty} a_n x^n / n!$ and $g(x) = \sum_{n=0}^{\infty} b_n x^n / n!$ be power series with a_n and b_n integers. If p is a prime such that $p \nmid a_i$ for $i = 0, \dots, p-1$, show that each coefficient c_t of the product $f(x)g(x) = \sum_{n=0}^{\infty} c_n x^n$ for $t = 0, \dots, p-1$ may be written in the form $p(A/B)$, $p \nmid B$.

Proof. Let $k \in \mathbb{N}, 0 \leq k \leq p-1$.

$$\begin{aligned} c_k &= \sum_{i+j=k} \frac{a_i}{i!} \frac{b_j}{j!} \\ &= \sum_{i=0}^k \frac{a_i}{i!} \frac{b_{k-i}}{(k-i)!} \\ &= \frac{1}{k!} \sum_{i=0}^k \binom{k}{i} a_i b_{k-i} \end{aligned}$$

As $k! \wedge p = 1$, and $\sum_{i=0}^k \binom{k}{i} a_i b_{k-i} \equiv 0 \pmod{p}$ for $k = 0, 1, \dots, p-1$,
 $c_k = p(A/B), p \wedge B = 1$. □

Ex. 6.22 Show that the relation $\varepsilon \equiv 1 \pmod{p}$ in Proposition 6.4.4 can also be achieved by replacing x by $1+t$ instead of e^z .

Proof. (solution given by agrounds)

We know from the remark after Prop 6.4.3 that

$$g(\chi) = \varepsilon \prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)}),$$

where $\varepsilon = \pm 1$. Let

$$f(x) = \sum_{j=1}^{p-1} \chi(j) x^j - \varepsilon \prod_{k=1}^{(p-1)/2} (x^{2k-1} - x^{p-(2k-1)}).$$

Then $f(0) = 0$ and $f(\zeta) = 0$, so $(x^p - 1)$ divides $f(x)$. As $f(x) \in \mathbb{Z}[x]$ and $x^p - 1 \in \mathbb{Z}[x]$ is monic, $f(x) = (x^p - 1)h(x)$, $h(x) \in \mathbb{Z}[x]$. If we replace x by $1+t$, we obtain

$$f(1+t) = \sum_{j=1}^{p-1} \chi(j)(1+t)^j - \varepsilon \prod_{k=1}^{(p-1)/2} \left((1+t)^{2k-1} - (1+t)^{p-(2k-1)} \right).$$

We compute the coefficient of $t^{(p-1)/2}$ in the polynomial $f(1+t)$:

$$\begin{aligned} \sum_{j=1}^{p-1} \chi(j)(1+t)^j &= \sum_{j=1}^{p-1} \chi(j) \sum_{i=1}^j \binom{j}{i} t^i \\ &= \sum_{i=1}^{p-1} \sum_{j=i}^{p-1} \chi(j) \binom{j}{i} t^i \end{aligned}$$

So the coefficient of $t^{(p-1)/2}$ in $\sum_{j=1}^{p-1} \chi(j)(1+t)^j$ is $\sum_{j=(p-1)/2}^{p-1} \chi(j) \binom{j}{(p-1)/2}$.

$$\begin{aligned} \prod_{k=1}^{(p-1)/2} ((1+t)^{2k-1} - (1+t)^{p-(2k-1)}) &= \prod_{k=1}^{(p-1)/2} ((1+(2k-1)t) - (1+(p-(2k-1))t + t^2 u(t))) \\ &= \prod_{k=1}^{(p-1)/2} ((4k-2-p)t + t^2 v(t)) \\ &= t^{(p-1)/2} \left(\prod_{k=1}^{(p-1)/2} (4k-2-p) \right) + t^{(p+1)/2} w(t), \end{aligned}$$

where $u(t), v(t), w(t)$ are polynomials. So the coefficient of $t^{(p-1)/2}$ in $f(1+t)$ is

$$c_{(p-1)/2} = \sum_{j=(p-1)/2}^{p-1} \chi(j) \binom{j}{(p-1)/2} - \varepsilon \prod_{k=1}^{(p-1)/2} (4k-2-p).$$

Furthermore,

$$\begin{aligned} f(1+t) &= ((1+t)^p - 1) h(1+t) \\ &= \left[\sum_{i=1}^p \binom{p}{i} t^i \right] h(1+t) \\ &= \left[\sum_{i=1}^p i! \binom{p}{i} \frac{t^i}{i!} \right] h(1+t) \\ &= \left[\sum_{i=0}^p a_i \frac{t^i}{i!} \right] h(1+t), \end{aligned}$$

where $a_0 = 0, a_i = i! \binom{p}{i} = \frac{p!}{(p-i)!}$, so $p \mid a_i, i = 0, \dots, p-1$: the conditions of Ex.21 are verified, so $f(1+t) = \sum_{i=0}^{p-1} c_i t^i$ is such that $c_{(p-1)/2} = p(A/B)$, $p \nmid B$. Equating these two evaluations of $c_{(p-1)/2}$, we obtain

$$\sum_{j=(p-1)/2}^{p-1} \chi(j) \binom{j}{(p-1)/2} - \varepsilon \prod_{k=1}^{(p-1)/2} (4k-2-p) = p \frac{A}{B}, \quad p \nmid B.$$

Multiplying by $B(p-1)!/2$, we obtain, as $p \nmid B$,

$$\begin{aligned} \frac{(p-1)!}{2} \sum_{j=(p-1)/2}^{p-1} \chi(j) \binom{j}{(p-1)/2} &\equiv \varepsilon \frac{(p-1)!}{2} \prod_{k=1}^{(p-1)/2} (4k-2) \\ &\equiv \varepsilon (2 \cdot 4 \cdot 6 \cdots (p-1)) \prod_{k=1}^{(p-1)/2} (2k-1) \equiv \varepsilon (p-1)! \\ &\equiv -\varepsilon \pmod{p} \end{aligned}$$

To prove that $\varepsilon = +1$, it remains to prove

$$\left(\frac{(p-1)}{2}\right)! \sum_{j=(p-1)/2}^{p-1} \chi(j) \binom{j}{(p-1)/2} \equiv -1 \pmod{p}$$

The factor of $((p-1)/2)!$ cancels the denominator of $\binom{j}{(p-1)/2}$, which leaves

$$\begin{aligned} & \sum_{j=(p-1)/2}^{p-1} \chi(j) \cdot j(j-1) \cdots \left(j - \frac{p-1}{2} + 1\right) \\ &= \sum_{j=1}^{p-1} \chi(j) \cdot j(j-1) \cdots \left(j - \frac{p-1}{2} + 1\right). \end{aligned}$$

The equality is justified because all terms for $j < \frac{p-1}{2}$ are zero. Collecting powers of j , this is

$$\sum_{j=1}^{p-1} \sum_{k=0}^{(p-1)/2} \chi(j) a_k j^k \equiv \sum_{k=0}^{(p-1)/2} a_k \sum_{j=1}^{p-1} j^{k+\frac{p-1}{2}} \pmod{p}$$

for some integers a_k . It's important to note that $a_{(p-1)/2} = 1$.

Now, we compute $\sum_{j=1}^{p-1} j^n \pmod{p}$. Let S denote this sum and let g be a generator of \mathbb{Z}/p^\times . Then

$$g^n S = \sum_{j=1}^{p-1} (gj)^n \equiv \sum_{j=1}^{p-1} j^n = S \pmod{p}.$$

Congruence holds because gj also runs over a complete system of nonzero residues mod p . If $g^n \neq 1$, then $S \equiv 0$. If $g^n \equiv 1$, then $j^n \equiv 1$ for all j , hence $S \equiv p-1 \equiv -1$.

Returning to the previous sum, the only nonzero term modulo p is $k = \frac{p-1}{2}$, so

$$\equiv \sum_{k=0}^{(p-1)/2} a_k \sum_{j=1}^{p-1} j^{k+\frac{p-1}{2}} \equiv a_{(p-1)/2} \cdot (-1) = -1 \pmod{p}$$

as desired. \square

Ex. 6.23 If $f(x) = x^n + a_1 x^{n-1} + \dots + a_n$, $a_i \in \mathbb{Z}$, and p is prime such that $p \mid a_i$ for $i = 1, \dots, n$, and $p^2 \nmid a_n$, show that $f(x)$ is irreducible over \mathbb{Q} (Eisenstein's irreducibility criterion).

Lemma. If $f \in \mathbb{Z}[x]$, $\deg(f) \geq 1$, is not irreducible in $\mathbb{Q}[x]$, then there exist $g, h \in \mathbb{Z}[x]$, $\deg(g) \geq 1$, $\deg(h) \geq 1$ such that $f = gh$.

Proof. (lemma) Suppose that $f(x) = \sum_{k=0}^n a_k x^k$, $a_k \in \mathbb{Z}$, is not irreducible in $\mathbb{Q}[x]$.

Then $f(x) = f_1(x)f_2(x)$, with $f_1, f_2 \in \mathbb{Q}[X]$, and $\deg(f_1) \geq 1$, $\deg(f_2) \geq 1$. As in Ex. 6.5, we can write $f_1(x) = \lambda p(x)$, $f_2(x) = \mu q(x)$ where $\lambda, \mu \in \mathbb{Q}$, and $p, q \in \mathbb{Z}[X]$ are primitive. Let $\nu = \lambda\mu \in \mathbb{Q}$: write $\nu = u/v$, $u \wedge v = 1$, $v \geq 1$. Then $r(x) = p(x)q(x) = \sum_{k=0}^n c_k x^k$ is primitive (Ex. 6.4), and $f(x) = \frac{u}{v} r(x) = \frac{u}{v} p(x)q(x)$.

As $vf(x) = ur(x)$, $v \mid uc_i$, $i = 0, 1, \dots, n$, with $u \wedge v = 1$, so $u \mid c_i$ for all i . The polynomial r being primitive, $v \mid 1$, so $v = \varepsilon = \pm 1$.

Let $g(x) = \varepsilon up(x)$, $h(x) = q(x)$. Then $g, h \in \mathbb{Z}[x]$, $\deg(g) \geq 1$, $\deg(h) \geq 1$, and $f = gh$ is the product of two non constant polynomials in $\mathbb{Z}[x]$. □

Proof. (Ex. 6.23)

Let

$$\varphi: \begin{cases} \mathbb{Z}[x] & \rightarrow \mathbb{F}_p[x] \\ p(x) = a_0 + \cdots + a_n x^n & \mapsto \bar{p}(x) = \bar{a}_0 + \cdots + \bar{a}_n x^n, \end{cases}$$

where \bar{a}_i is the class of a_i in \mathbb{F}_p . φ is a ring homomorphism.

We show that $f(x) = g(x)h(x)$, $g, h \in \mathbb{Z}[x]$, $\deg(g) \geq 1$, $\deg(h) \geq 1$ is impossible. Indeed in such a situation,

$$\bar{f}(x) = x^n = \bar{g}(x)\bar{h}(x).$$

As the only irreducible factor of x^n is x , the unicity of the decomposition of a polynomial in irreducible factors in $\mathbb{F}_p[x]$ gives

$$\bar{g}(x) = \lambda x^i, \bar{h}(x) = \mu x^j, \lambda, \mu \in \mathbb{F}_p, i, j \in \mathbb{N}.$$

As $\deg(\bar{g}) \leq \deg(g)$, $\deg(\bar{h}) \leq \deg(h)$ and $\deg(\bar{g}) + \deg(\bar{h}) = n = \deg(f) + \deg(g)$, this implies that $i = \deg(\bar{f}) = \deg(f)$, $j = \deg(\bar{g}) = \deg(g)$, so $i \geq 1, j \geq 1$. Therefore $p \mid g(0), p \mid h(0)$, so $p^2 \mid a_n = g(0)h(0)$, which is in contradiction with the hypothesis.

From the lemma we deduce that $f(x)$ is irreducible in $\mathbb{Q}[x]$. □