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

Richard Ganaye

September 17, 2019

1 Chapter 1

Ex 1.1 *Let a and b be nonzero integers. We can find nonzero integers q and r such that $a = qb + r$ where $0 \le r < b$. Prove that $(a, b) = (b, r)$.*

Proof. Notation : if a, b are integers in $\mathbb{Z}$, $a \wedge b$ is the non negative greatest common divisor of a, b, the generator in $\mathbb{N} = \{0, 1, 2, \ldots\}$ of the ideal $(a, b) = a\mathbb{Z} + b\mathbb{Z}$.

Let $d \in \mathbb{Z}$.
• If $d \mid a, d \mid b$, then $d \mid a - qb = r$, so $d \mid b, d \mid r$.
• If $d \mid b, d \mid r$, then $d \mid qb + r = a$, so $d \mid a, d \mid b$.

$$\forall d \in \mathbb{Z},\ (d \mid b, d \mid r) \iff (d \mid a, d \mid b).$$

If $a = bq + r$, the set of common divisors of a, b is equal to the set of common divisors of b, r.

As $a \wedge b$ is the smallest positive element of this set, so is $b \wedge r$, we conclude that $a \wedge b = b \wedge r$. □

Ex 1.2 *If $r \neq 0$, we can find q_1 and r_1 such that $b = q_1 r + r_1$, with $0 \le r_1 < r$. Show that $(a, b) = (r, r_1)$. This process can be repeated. Show that it must end in finitely many steps. Show that the last nonzero remainder must equal (a, b). The process looks like*

$$\begin{aligned}
a &= bq + r, & 0 &\le r < b \\
b &= q_1 r + r_1, & 0 &\le r_1 < r \\
r &= q_2 r_1 + r_2, & 0 &\le r_2 < r_1 \\
&\vdots \\
r_{k-1} &= q_{k+1} r_k + r_{k+1}, & 0 &\le r_{k+1} < r_k \\
r_k &= q_{k+2} r_{k+1}
\end{aligned}$$

Then $r_{k+1} = (a, b)$. This process of finding (a, b) is known as the Euclidian algorithm.

Proof. The Euclidian division of b by r gives $b = q_1 r + r_1, 0 \le r_1 < r$. The result of exercise 1.1 applied to the couple (b, r) shows that

$$b \wedge r = r \wedge r_1.$$

Let $N \in \mathbb{N}$. While the remainders $r_i, i \leq N$, are not equal to 0, we can define the sequences $(q_i), (r_i)$ by

$$r_{-1} = a, r_0 = b, \qquad r_{i-1} = q_{i+1} r_i + r_{i+1},\ 0 \leq r_{i+1} < r_i \quad 0 \leq i \leq N$$

.

If no $r_i, i \in \mathbb{N}$, is equal to 0, we can continue this construction indefinitely. So we obtain a strictly decreasing sequence $(r_i)_{i\in\mathbb{N}}$ of positive numbers : it is impossible. Therefore, there exists an index k such as $r_{k+2} = 0$, this is the end of the algorithm.

$$\begin{aligned}
a &= bq + r, & 0 \leq r < b \\
b &= q_1 r + r_1, & 0 \leq r_1 < r \\
r &= q_2 r_1 + r_2, & 0 \leq r_2 < r_1 \\
&\vdots \\
r_{k-1} &= q_{k+1} r_k + r_{k+1}, & 0 \leq r_{k+1} < r_k \\
r_k &= q_{k+2} r_{k+1}, & r_{k+2} = 0
\end{aligned}$$

From exercise 1, $r_{i-1} \wedge r_i = r_i \wedge r_{i+1}, 0 \leq i \leq k$, so

$$a \wedge b = b \wedge r = \cdots = r_k \wedge r_{k+1} = r_{k+1} \wedge r_{k+2} = r_{k+1} \wedge 0 = r_{k+1}.$$

The last non zero remainder is the gcd of a, b. □

Ex 1.3 *Calculate* $(187, 221)$, $(6188, 4709)$, $(314, 159)$.

Proof. With direct instructions in Python, we obtain :

```
>>> a, b = 187,  221
>>> print("q = ",a//b); a, b = b, a%b; print(a,b)
q =  0
221 187
>>> print("q = ",a // b); a, b = b, a%b; print(a,b)
q =  1
187 34
>>> print("q = ",a // b); a, b = b, a%b; print(a,b)
q =  5
34 17
>>> print("q = ",a // b); a,b = b, a%b; print(a,b)
q =  2
17 0
```

This gives the equalities

$$\begin{aligned}
187 &= 0 \times 221 + 187 \\
221 &= 1 \times 187 + 34 \\
187 &= 5 \times 34 + 17 \\
34 &= 2 \times 17 + 0
\end{aligned}$$

So $187 \wedge 221 = 17$.

With the same instructions, we obtain

$$\begin{aligned}
6188 &= 1 \times 4709 + 1479\\
4709 &= 3 \times 1479 + 272\\
1479 &= 5 \times 272 + 119\\
272 &= 2 \times 119 + 34\\
119 &= 3 \times 34 + 17\\
34 &= 2 \times 17 + 0
\end{aligned}$$

$6188 \wedge 4709 = 17$.

Finally

$$\begin{aligned}
314 &= 1 \times 159 + 155\\
159 &= 1 \times 155 + 4\\
155 &= 38 \times 4 + 3\\
4 &= 1 \times 3 + 1\\
3 &= 3 \times 1 + 0
\end{aligned}$$

$314 \wedge 159 = 1$.

The Python script which gives the gcd is very concise :

```
def gcd(a,b):
    a, b = abs(a), abs(b)
    while b != 0:
        a, b = b, a % b
    return a
```

□

Ex 1.4 *Let $d = (a, b)$. Show how one can use the Euclidean algorithm to find numbers m and n such that $am + bn = d$.(Hint: In Exercise 2 we have that $d = r_{k+1}$. Express r_{k+1} in terms of r_k and r_{k+1}, then in terms of r_{k-1} and r_{k-2}, etc.).*

Proof. With a slight modification of the notations of exercise 2, we note the Euclid's algorithm under the form

$$r_0 = a, r_1 = b, \qquad r_i = r_{i+1}q_{i+1} + r_{i+2}, \quad 0 < r_{i+2} < r_{i+1},\ 0 \leq i < k, \quad r_k = q_{k+1}r_{k+1},\ r_{k+2} = 0$$

We show by induction on i $(i \leq k+1)$ the proposition

$$P(i) : \exists (m_i, n_i) \in \mathbb{Z} \times \mathbb{Z},\ r_i = am_i + bn_i.$$

- $r_0 = a = 1.a + 0.b$. Define $m_0 = 1, n_0 = 0$. We obtain $r_0 = am_0 + bn_0$, then $P(0)$ is true.

$r_1 = b = 0.a + 1.b$. Define $m_1 = 0, n_1 = 1$. We obtain $r_1 = am_1 + bn_1$, then $P(1)$ is true.

• Suppose for $0 \leq i < k$ the induction hypothesis $P(i)$ et $P(i+1)$:

$$\begin{aligned} r_i &= am_i + bn_i, & m_i, n_i \in \mathbb{Z}, \\ r_{i+1} &= am_{i+1} + bn_{i+1}, & m_{i+1}, n_{i+1} \in \mathbb{Z}. \end{aligned}$$

Then $r_{i+2} = r_i - r_{i+1}q_{i+1} = a(m_i - q_{i+1}m_{i+1}) + b(n_i - q_{i+1}n_{i+1})$.

If we define $m_{i+1} = m_i - q_{i+1}m_{i+1}, n_{i+1} = n_i - q_{i+1}n_{i+1}$, we obtain $r_{i+2} = am_{i+2} + bn_{i+2},\ m_{i+2}, n_{i+2} \in \mathbb{Z}$, so $P(i+2)$.

• The conclusion is that $P(i)$ is true for all $i, 0 \leq i \leq k+1$, in particular $r_{k+1} = am_{k+1} + bn_{k+1}$, that is

$$a \wedge b = d = am + bn,$$

where $m = m_{k+1}, n = n_{k+1} \in \mathbb{Z}$. □

Ex 1.5 *Find m and n for the pairs a and b given in Ex 1.3*

Proof. From exercises 1.3, 1.4, we know that the sequences $(r_i), (m_i), (n_i)$ are given by

$$\begin{aligned} r_0 &= a, r_1 = b \\ m_0 &= 1, m_1 = 0 \\ n_0 &= 0, n_1 = 1 \end{aligned}$$

and for all $i < k$,

$$\begin{aligned} r_{i+2} &= r_i - q_{i+1}r_{i+1} \\ m_{i+2} &= m_i - q_{i+1}m_{i+1} \\ n_{i+2} &= n_i - q_{i+1}n_{i+1} \end{aligned}$$

and for all i

$$r_i = m_i a + n_i b.$$

This gives the direct instructions in Python :

```
>>> a,b = 187, 221
>>> r0,r1,m0,m1,n0,n1 = a,b,1,0,0,1
>>> q = r0//r1;
>>> q = r0//r1; r0,r1,m0,m1,n0,n1 = r1, r0 -q*r1,m1, m0 -q*m1, n1, n0 - q*n1
>>> print(r0,r1,m0,m1,n0,n1)
221 187 0 1 1 0
>>> q = r0//r1; r0,r1,m0,m1,n0,n1 = r1, r0 -q*r1,m1, m0 -q*m1, n1, n0 - q*n1
>>> print(r0,r1,m0,m1,n0,n1)
187 34 1 -1 0 1
>>> q = r0//r1; r0,r1,m0,m1,n0,n1 = r1, r0 -q*r1,m1, m0 -q*m1, n1, n0 - q*n1
>>> print(r0,r1,m0,m1,n0,n1)
34 17 -1 6 1 -5
>>> q = r0//r1; r0,r1,m0,m1,n0,n1 = r1, r0 -q*r1,m1, m0 -q*m1, n1, n0 - q*n1
>>> print(r0,r1,m0,m1,n0,n1)
17 0 6 -13 -5 11
```

So

$$17 = 187 \wedge 221 = 6 \times 187 - 5 \times 221.$$

Similarly

$$17 = 6188 \wedge 4709 = 121 \times 6188 - 159 \times 4709.$$

$$1 = 314 \wedge 159 = -40 \times 314 + 79 \times 159.$$

We obtain the same results with the following Python script :

```
def bezout(a,b):
    """input  : entiers a,b
        output : tuple (x,y,d),
        (x,y) solution de ax+by = d, d = pgcd(a,b)
    """
    (r0,r1)=(a,b)
    (u0,v0) = (1,0)
    (u1,v1) = (0,1)
    while r1 != 0:
        q = r0 // r1
        (r2,u2,v2) = (r0 - q*r1,u0 - q*u1,v0 - q*v1)
        (r0,r1) = (r1,r2)
        (u0,u1) = (u1,u2)
        (v0,v1) = (v1,v2)
    return (u0,v0,r0)
```

$\square$

Ex 1.6 *Let $a, b, c \in \mathbb{Z}$. Show that the equation $ax + by = c$ has solutions in integers iff $(a, b)|c$.*

Proof. Let $d = a \wedge b$.

- If $ax + by = c, x, y \in \mathbb{Z}$, as $d \mid a, d \mid b$, $d \mid ax + by = c$.
- Reciprocaly, if $d \mid c$, then $c = dc'$, $c' \in \mathbb{Z}$.

From Prop. 1.3.2., $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, so $d = au + bv$, $u, v \in \mathbb{Z}$, and $c = dc' = a(c'u) + b(c'v) = ax + by$, where $x = c'u, y = c'v$ are integers.

Conclusion :

$$\exists (x, y) \in \mathbb{Z} \times \mathbb{Z},\ ax + by = c \iff a \wedge b \mid c.$$

$\square$

Ex 1.7 *Let $d = (a, b)$ and $a = da'$ and $b = db'$. Show that $(a', b') = 1$.*

Proof. Suppose $d \neq 0$ (if $d = 0$, then $a = b = 0$, and a', b' are any numbers in $\mathbb{Z}$ and the result may be false, so we must suppose $d \neq 0$).

As $d = am+bn$, $m, n \in \mathbb{Z}$, $d = d(a'm+b'n)$, so $1 = a'm+b'n$, which proves $a' \wedge b' = 1$.

conclusion : if $d = a \wedge b \neq 0$, and $a = da', b = db'$, then $a' \wedge b' = 1$.

$\square$

Ex. 1.8 *Let x_0 and y_0 be a solution to $ax+by=c$. Show that all solutions have the form $x = x_0 + t(b/d)$, $y = y_0 - t(a/d)$, where $d = (a,b)$ and $t \in \mathbb{Z}$.*

Proof. Suppose $a \neq 0, b \neq 0$.

Let x_0 and y_0 be a solution to $ax+by=c$.

If (x,y) is any solution of the same equation,

$$\begin{aligned} ax+by &= c\\ ax_0+by_0 &= c, \end{aligned}$$

then

$$a(x-x_0) = -b(y-y_0),$$

so

$$\frac{a}{d}(x-x_0) = -\frac{b}{d}(y-y_0).$$

Let $a' = a/d, b' = b/d$: from ex. 1.7, we know that $a' \wedge b' = 1$.

As $a'(x-x_0) = -b'(y-y_0)$, $b' \mid a'(x-x_0)$, and $b' \wedge a' = 1$, so (Gauss' Lemma : prop. 1.1.1) $b' \mid x - x_0$.

There exists $t \in \mathbb{Z}$ such that $x - x_0 = tb'$. Then $a'tb' = -b'(y-y_0)$. As $b \neq 0$, $b' \neq 0$, so $a't = -(y-y_0)$:

$$\begin{aligned} x &= x_0 + t(b/d)\\ y &= y_0 - t(a/d) \end{aligned}$$

Reciprocaly, $a(x_0 + t(b/d)) + b(y_0 - t(a/d)) = ax_0 + by_0 = c$.

Conclusion : if $a \neq 0, b \neq 0$, and $ax_0 + by_0 = c$,

$$ax+by=c \iff \exists t \in \mathbb{Z},\ x = x_0 + t(b/d), y = y_0 - t(a/d).$$

□

Ex. 1.9 *Suppose that $u, v \in \mathbb{Z}$ and that $(u,v) = 1$. If $u \mid n$ and $v \mid n$, show that $uv \mid n$. Show that this is false if $(u,v) \neq 1$.*

Proof. As $u \mid n$, $n = uq, q \in \mathbb{Z}$, so $v \mid n = uq$, and $v \wedge u = 1$, so (Gauss' lemma : prop. 1.1.1), $v \mid q$: $q = vl, l \in \mathbb{Z}$, and $n = uvl$: $uv \mid n$.

If the case $u \wedge v \neq 1$, we give the counterexample $6 \mid 18, 9 \mid 18$, but $6 \times 9 \nmid 18$. □

Ex. 1.10 *Suppose that $(u,v) = 1$. Show that $(u+v, u-v)$ is either 1 or 2.*

Proof. Let $d = (u+v) \wedge (u-v)$. Then $d \mid u+v, d \mid u-v$, so $d \mid 2u = (u+v)+(u-v)$ and $d \mid 2v = (u+v)-(u-v)$. So $d \mid (2u) \wedge (2v) = 2(u \wedge v) = 2$. As $d \geq 0$, $d = 1$ or $d = 2$. □

Ex. 1.11 *Show that $(a, a+k) \mid k$.*

Proof. Let $d = a \wedge (a+k)$. As $d \mid a, d \mid (a+k)$, $d \mid k = (a+k) - a$.

Conclusion : $a \wedge (a+k) \mid k$. □

Ex. 1.12 *Suppose that we take several copies of a regular polygon and try to fit them evenly about a common vertex. Prove that the only possibilities are six equilateral triangles, four squares, and three hexagons.*

Proof. Let n be the number of sides of the regular polygon, m the number of sides starting from a summit in the lattice, α the measure of the exterior angle, β the measure of the interior angle (in radians) $(\alpha+\beta=\pi)$.

Then $\alpha = 2\pi/n, \beta = \pi - 2\pi/n$.

$m\beta = 2\pi, m(\pi - 2\pi/n) = 2\pi, m(1-2/n) = 2$, so

$$\frac{1}{m} + \frac{1}{n} = \frac{1}{2}, \qquad m > 0, n > 0. \tag{1}$$

As this equation is symmetric in m, n, we may suppose first $m \le n$.

In this case $1/m \ge 1/n$, so $2/n \le 1/2 : n \ge 4$.

If $n > 6$, $1/n < 1/6, 1/m = 1/2 - 1/n > 1/2 - 1/6 = 1/3$, so $m < 3, m \le 2 : m = 1$ or $m = 2$.

If $m = 1$, $n < 0 :$ it is impossible. If $m = 2$, $1/n = 0 :$ also impossible. Therefore $n \le 6 : 4 \le n \le 5$. If $n = 4, m = 4$. if $n = 5$, $n = 10/3 :$ impossible. if $n = 6$, $m = 3$. Using the symetry, the set of solutions of (1) is

$$S = \{(3,6), (6,3), (4,4)\},$$

corresponding with the usual lattices composed of equilateral triangles, squares or hexagons. $\square$

Ex. 1.13 *Let $n_1, n_2, \ldots, n_s \in \mathbb{Z}$. Define the greatest common divisor d of $n_1, n_2, \ldots, n_s$ and prove that there exist integers $m_1, m_2, \ldots, m_s$ such that $n_1m_1 + n_2m_2 \cdots + n_sm_s = d$.*

Proof. Let $n_1, n_2, \ldots, n_s \in \mathbb{Z}$. The ideal of $\mathbb{Z}$, $(n_1, \ldots, n_s) = n_1\mathbb{Z} + \cdots + n_s\mathbb{Z}$ is principal, so there exists an unique $d \in \mathbb{Z}, d \ge 0$ such that

$$n_1\mathbb{Z} + \cdots + n_s\mathbb{Z} = d\,\mathbb{Z} \quad (d \ge 0).$$

We define

$$d = \gcd(n_1, \ldots, n_s) \iff n_1\mathbb{Z} + \cdots + n_s\mathbb{Z} = d\,\mathbb{Z} \text{ and } d \ge 0. \tag{2}$$

The characterization of the gcd is

$$d = \gcd(n_1, \ldots, n_s) \iff$$

$$(i)\ d \ge 0 \tag{3}$$
$$(ii)\ d \mid n_1, \ldots, d \mid n_s \tag{4}$$
$$(iii)\ \forall \delta \in \mathbb{Z},\ (\delta \mid n_1, \ldots, \delta \mid n_s) \Rightarrow \delta \mid d \tag{5}$$

($\Rightarrow$) Indeed, if we suppose (1), then $d \ge 0$, and $n_1 = n_1.1 + n_2.0 + \cdots + n_s.0 \in n_1\mathbb{Z} + \cdots + n_s\mathbb{Z} = d\,\mathbb{Z}$, so $d \mid n_1$. Similarly $d \mid n_i, 1 \le i \le s$ so (i)(ii) are true. if $\delta \mid n_i, 1 \le i \le s$, as $d = n_1m_1 + \cdots + n_sm_s, m_1, \ldots, m_s \in \mathbb{Z}$, then $\delta \mid d$.

($\Leftarrow$) Suppose that d verify (i)(ii)(iii). From (ii), we see that $n_i\mathbb{Z} \subset d\mathbb{Z}, i = 1, \ldots, s$, so $n_1\mathbb{Z} + \cdots + n_s\mathbb{Z} \subset d\mathbb{Z}$.

As $\mathbb{Z}$ is a principal ring, there exists $\delta \geq 0$ such that $n_1\mathbb{Z} + \cdots + n_s\mathbb{Z} = \delta\,\mathbb{Z}$. $n_i \in n_1\mathbb{Z}+\cdots+n_s\mathbb{Z}$ so $n_i \in \delta\mathbb{Z},\ i = 1,\ldots,s : \delta \mid n_1,\ldots,\delta \mid n_s$. From (iii), we deduce $\delta \mid d$. As $\delta\mathbb{Z} \subset d\mathbb{Z}$, $d \mid \delta$, with $d \geq 0, \delta \geq 0$. Consequently, $d = \delta$ and $n_1\mathbb{Z} + \cdots + n_s\mathbb{Z} = d\,\mathbb{Z}, d \geq 0$, so $d = \gcd(n_1,\ldots,n_s)$.

At last, as $n_1\mathbb{Z} + \cdots + n_s\mathbb{Z} = d\,\mathbb{Z}$, there exist integers $m_1, m_2, \ldots, m_s$ such that $n_1m_1 + n_2m_2 + \cdots + n_sm_s = d$. $\square$

Ex. 1.14 *Discuss the solvability of $a_1x_1 + a_2x_2 + \cdots + a_rx_r = c$ in integers. (Hint: Use Exercise 13 to extend the reasoning behind Exercise 6.)*

Proof. Let $a_1, a_2, \ldots, a_r \in \mathbb{Z}$.

Note $\gcd(a_1, a_2, \ldots, a_r) = a_1 \wedge a_2 \wedge \cdots \wedge a_r$. The following result generalizes Ex. 6 :

$$\exists (x_1, x_2, \ldots, x_r) \in \mathbb{Z}^r,\ a_1x_1 + a_2x_2 + \cdots + a_rx_r = c \iff a_1 \wedge a_2 \wedge \cdots \wedge a_r \mid c.$$

Let $d = a_1 \wedge a_2 \wedge \cdots \wedge a_r$.

- If $a_1x_1 + a_2x_2 + \cdots + a_rx_r = c$, as $d \mid a_1, \ldots, d \mid a_r$, $d \mid a_1x_1 + a_2x_2 + \cdots + a_rx_r = c$.
- Reciprocaly, if $d \mid c$, then $c = dc', c' \in \mathbb{Z}$.

As $d\mathbb{Z} = a_1\mathbb{Z}+a_2\mathbb{Z}+\cdots+a_r\mathbb{Z}$, so $d = a_1m_1+a_2m_2+\cdots+a_rm_r,\ m_1, m_2, \ldots, m_r \in \mathbb{Z}$. $c = dc' = a_1(m_1c')+\cdots a_r(m_rc') = a_1x_1+\cdots+a_rx_r$, where $x_i = m_ic', i = 1, 2, \ldots, r$. $\square$

Ex. 1.15 *Prove that $a \in \mathbb{Z}$ is the square of another integer iff $\mathrm{ord}_p(a)$ is even for all primes p. Give a generalization.*

Proof. Suppose $a = b^2, b \in \mathbb{Z}$. Then $\mathrm{ord}_p(a) = 2\,\mathrm{ord}_p(b)$ is even for all primes p.

Reciprocally, suppose that $\mathrm{ord}_p(a)$ is even for all primes p. We must also suppose $a > 0$. Let $a = \prod_p p^{a(p)}$ the decomposition of a in primes. As $a(p)$ is even, $a(p) = 2b(p)$ for an integer $b(p)$ function of the prime p. Let $b = \prod_p p^{b(p)}$. Then $a = b^2$.

With a similar demonstration, we obtain the following generalization for each integer $a \in \mathbb{Z}, a > 0$:

$a = b^n$ for an integer $b \in \mathbb{Z}$ iff $n \mid \mathrm{ord}_p(a)$ for all primes p. $\square$

Ex. 1.16 *If $(u, v) = 1$ and $uv = a^2$, show that both u and v are squares.*

Proof. Here $u, v \in \mathbb{N}$, where $\mathbb{N} = \{0, 1, 2, \ldots\}$.

For all primes p such that $p \mid u$, $\mathrm{ord}_p(u) + \mathrm{ord}_p(v) = 2\ \mathrm{ord}_p(a)$. As $u \wedge v = 1$ and $p \mid u$, $p \nmid v$, so $\mathrm{ord}_p(v) = 0$. Consequently, $\mathrm{ord}_p(u)$ is even for all prime p such that $p \mid u$. From Exercise 1.15, we can conclude that u is a square. Similarly, v is a square. $\square$

Ex. 1.17 *Prove that the square root of 2 is irrational, i.e., that there is no rational number $r = a/b$ such that $r^2 = 2$.*

Proof. Suppose there exists $r \in \mathbb{Q}, r > 0$ such that $r^2 = 2$. Then $r = a/b, a \in \mathbb{N}^*, b \in \mathbb{N}^*$. With $d = a \wedge b$, $a = da', b = db', a' \wedge b' = 1$, so $r = a'/b', a' \wedge b' = 1$, so we may suppose $r = a/b, a > 0, b > 0, a \wedge b = 1$ and $a^2 = 2b^2$.

a^2 is even, then a is even (indeed, if a is odd, $a = 2k + 1, k \in \mathbb{Z}$, $a^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ is odd).

So $a = 2A, A \in \mathbb{N}$, then $4A^2 = 2b^2$, $2A^2 = b^2$.

With the same reasoning, b^2 is even, then b is even : $b = 2B, B \in \mathbb{N}$. $2 \mid a, 2 \mid b$, $2 \mid a \wedge b$, in contradiction with $a \wedge b = 1$.

Conlcusion : $\sqrt{2}$ is irrational. $\square$

Ex. 1.18 *Prove that $\sqrt[n]{m}$ is irrational if m is not the n-th power of an integer.*

Proof. Here $m \in \mathbb{N}$.

Suppose that $r = \sqrt[n]{m} \in \mathbb{Q}$. As $r \geq 0$, $r = a/b, a \geq 0, b > 0, a \wedge b = 1$, and $r^n = m$, so $a^n = mb^n$.

For all primes p, $n \operatorname{ord}_p(a) = \operatorname{ord}_p(m) + n \operatorname{ord}_p(b)$, so $n \mid \operatorname{ord}_p(m)$.

From Ex. 1.15, we conclude that m is a n-th power.

Conclusion : if $m \geq 0$ is not the n-th power of an integer, $\sqrt[n]{m}$ is irrational. $\square$

Ex. 1.19 *Define the least common multiple of two integers a and b to be an integer m such that $a \mid m$, $b \mid m$, and m divides every common multiple of a and b. Show that such an m exists. It is determined up to sign. We shall denote it by $[a, b]$.*

Proof. As $a\mathbb{Z} \cap b\mathbb{Z}$ is an ideal of $\mathbb{Z}$, and $\mathbb{Z}$ is a principal ideal domain, there exists an unique $m \geq 0$ such that $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. So by definition,

$$m = [a, b] \iff a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z} \text{ and } m \geq 0.$$

We may note also $[a, b] = a \vee b$.

characterization of lcm :

$$\begin{aligned} m = a \vee b \iff & \\ & (i)\ m \geq 0 \\ & (ii)\ a \mid m, b \mid m \\ & (iii)\ \forall \mu \in \mathbb{Z}, (a \mid \mu, b \mid \mu) \Rightarrow m \mid \mu \end{aligned}$$

($\Rightarrow$) By definition, $m \geq 0$. $m \in m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, so $a \mid m$ and $b \mid m$: (ii) is verified. If $\mu \in \mathbb{Z}$ is such that $a \mid \mu, b \mid \mu$, then $\mu \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, so $m \mid \mu$: (iii) is true.

($\Leftarrow$) Suppose that m verifies (i),(ii),(iii). Let m' such that $a\mathbb{Z} \cap b\mathbb{Z} = m'\mathbb{Z}, m' \geq 0$. We show that $m = m'$.

As $m' \in a\mathbb{Z} \cap b\mathbb{Z}, a \mid m', b \mid m'$, so from (iii) $m \mid m'$. From (ii), we see that $m \in a\mathbb{Z} \cap b\mathbb{Z} = m'\mathbb{Z}$, so $m' \mid m, m \geq 0, m' \geq 0$. The conclusion is $m = m'$ and $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}, m \geq 0$, so $m = a \vee b$. $\square$

Ex. 1.20 *Prove the following:*

(a) $\operatorname{ord}_p[a, b] = \max(\operatorname{ord}_p(a), \operatorname{ord}_p(b))$.

(b) $(a, b)[a, b] = ab$.

(c) $(a + b, [a, b]) = (a, b)$.

Proof. (a) Let $a = \varepsilon \prod_p p^{a(p)}, b = \varepsilon' \prod_p p^{b(p)}, \varepsilon, \varepsilon' = \pm 1$, and

$$m = \prod_p p^{\max(a(p), b(p))}.$$

Then

(i) $m \geq 0$.

(ii) As $a(p) \le \max(a(p), b(p))$, $p^{a(p)} \mid p^{\max(a(p),b(p))}$, so $a \mid m$. Similarly, $b \mid m$.

(iii) If $\mu = \varepsilon'' \prod_p p^{c(p)}$ is a common multiple of a and b, then for all primes p, $a(p) \le c(p), b(p) \le c(p)$, so $\max(a(p), b(p) \le c(p)$, so $m \mid \mu$. m verifies the characterisation of lcm :

$$m = a \vee b = \prod_p p^{\max(a(p),b(p))}.$$

So $\mathrm{ord}_p[a,b] = \max(\mathrm{ord}_p(a), \mathrm{ord}_p(b))$.

(b) Similarly, we prove that

$$a \wedge b = \prod_p p^{\min(a(p),b(p))}.$$

As $\max(a,b) + \min(a,b) = a + b$, we obtain

$$(a \vee b)(a \wedge b) = |ab|.$$

Second proof (without decompositions in primes) :

Let $d = a \wedge b$. If $d = 0$, then $a = b = 0$ and $(a \vee b)(a \wedge b) = ab$.

Suppose now that $d \ne 0$. There exist integers a', b' such that

$$a = da', b = db', a' \wedge b' = 1.$$

Let $m = da'b'$: $a = da' \mid m$ and $b = db' \mid m$. If μ is a common multiple of a and b, then $d \mid \mu$, and $a' \mid \mu/d, b' \mid \mu/d$. As $a' \wedge b' = 1$, $a'b' \mid \mu/d$ (see Ex.1.9). so $m = da'b' \mid \mu$.

$|m|$ verifies the characterization of lcm (Ex. 1.19), so $a \vee b = |m| = |da'b'| = |ab|/d$. Conclusion : $(a \vee b)(a \wedge b) = |ab|$.

(c) Let $\delta \in \mathbb{Z}$. If $\delta \mid a, \delta \mid b$, then $\delta \mid a + b$ and $\delta \mid a \vee b$.

Reciprocally, suppose that $\delta \mid a + b, \delta \mid a \vee b$.

Let $a', b' \in \mathbb{Z}$ such that $a = da', b = db', a' \wedge b' = 1$. Then $a \vee b = da'b'$, so

$$\begin{aligned} &\delta \mid d(a' + b'),\\ &\delta \mid da'b'. \end{aligned}$$

Multiplying the first relation by b' and a', we obtain : $\delta \mid da'b' + db'^2, \delta \mid da'^2 + da'b'$. As $\delta \mid da'b'$, we obtain :

$$\begin{aligned} &\delta \mid db'^2\\ &\delta \mid da'^2 \end{aligned}$$

As $a'^2 \wedge b'^2 = 1$, $\delta \mid d(a'^2 \wedge b'^2) = d$, so $\delta \mid a, \delta \mid b$.

The set of divisors of a, b is the same that the set of divisors of $a + b, a \vee b$, so

$$(a + b) \wedge (a \vee b) = a \wedge b.$$

□

Ex. 1.21 *Prove that* $\mathrm{ord}_p(a+b) \geq \min(\mathrm{ord}_p a, \mathrm{ord}_p b)$ *with equality holding if* $\mathrm{ord}_p a \neq \mathrm{ord}_p b$.

Proof. As $a \wedge b \mid a+b, \mathrm{ord}_p(a \wedge b) \leq \mathrm{ord}_p(a+b)$, so $\min(\mathrm{ord}_p(a), \mathrm{ord}_p(b)) \leq \mathrm{ord}_p(a+b)$.

Suppose $\mathrm{ord}_p(a) \neq \mathrm{ord}_p(b)$,The problem being symmetric in a, b, we may suppose $\alpha = \mathrm{ord}_p(a) < \beta = \mathrm{ord}_p(b)$. So there exist $q, r \in \mathbb{Z}$ such that

$$a = p^\alpha q,\ p \nmid q$$
$$b = p^\beta r,\ p \nmid r \qquad \alpha < \beta$$

Then $a + b = p^\alpha(q + p^{\beta-\alpha} r)$, where $p \nmid q + p^{\beta-\alpha} r$ (as $p \mid p^{\beta-\alpha}$ and $p \nmid q$).

So $\mathrm{ord}_p(a+b) = \alpha = \min(\mathrm{ord}_p(a), \mathrm{ord}_p(b))$. □

Ex. 1.22 *Almost all the previous exercises remain valid if instead of the ring* $\mathbb{Z}$ *we consider the ring* $k[x]$. *Indeed, in most we can consider any Euclidean domain. Convince yourself of this fact. For simplicity we shall continue to work in* $\mathbb{Z}$.

Proof. We can adapt all the preceding proofs to the Euclidean domain $k[x]$. The only difference is that the units in $\mathbb{Z}$ are ± 1, and the units in $k[x]$ are the elements of k^*. □

Ex. 1.23 *Suppose that* $a^2 + b^2 = c^2$ *with* $a, b, c \in \mathbb{Z}$ *For example,* $3^2 + 4^2 = 5^2$ *and* $5^2 + 12^2 = 13^2$. *Assume that* $(a, b) = (b, c) = (c, a) = 1$. *Prove that there exist integers* u *and* v *such that* $c - b = 2u^2$ *and* $c + b = 2v^2$ *and* $(u, v) = 1$ *(there is no loss in generality in assuming that* b *and* c *are odd and that* a *is even). Consequently* $a = 2uv$, $b = v^2 - u^2$, *and* $c = v^2 + u^2$. *Conversely show that if* u *and* v *are given, then the three numbers* a, b, *and* c *given by these formulas satisfy* $a^2 + b^2 = c^2$.

Proof. Suppose $x^2 + y^2 = z^2,\ x, y, z \in \mathbb{Z}$. Let $d = x \wedge y \wedge z$. If $d = 0$, then $x = y = z = 0$. If $d \neq 0$, and $a = x/d, b = y/d, c = z/d$, then $a^2 + b^2 = c^2$, with $a \wedge b \wedge c = 1$. If a prime p is such that $p \mid a, p \mid b$, then $p \mid c^2$, so $p \mid c$ (as p is a prime). Then $p \mid a \wedge b \wedge c = 1$: this is impossible, so $a \wedge b = 1$, and similarly $a \wedge c = 1, b \wedge c = 1$.

If a, b are odd, then $a^2 \equiv b^2 \equiv 1 \pmod 4$, so $c^2 \equiv 2 \pmod 4$. As the squares modulo 4 are $0, 1$, this is impossible. As $a \wedge b = 1$, a, b are not both even, so a, b are not of the same parity. Without loss of generality, we may exchange a, b so that a is even, b is odd, and then c is odd.

$a^2 = c^2 - b^2 = (c - b)(c + b)$, so

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

where $a/2, (c-b)/2, (c+b)/2$ are integers.

If $d \mid (c-b)/2$ and $d \mid (c+b)/2$, then $d \mid c = (c+b)/2 + (c-b)/2$, and $d \mid b = (c-b)/2 - (c-b)/2$, so $d \mid a \wedge b = 1$. This proves

$$\left(\frac{c+b}{2}\right) \wedge \left(\frac{c-b}{2}\right) = 1.$$

Using Ex. 1.16, we see that $(c+b)/2$ and $(c-b)/2$ are squares : there exist u, v such that

$$c - b = 2u^2, c + b = 2v^2, \qquad u \wedge v = 1.$$

$(a/2)^2 = u^2v^2$, and we can choose the signs of u, v such that $a = 2uv$. Then $b = v^2 - u^2, c = v^2 + u^2$. There exists $\lambda \in \mathbb{Z}$ ($\lambda = d$) such that $x = 2\lambda uv, y = \lambda(v^2 - u^2), z = \lambda(v^2 + u^2)$.

Conversely, if λ, u, v are any integers, $(2\lambda uv)^2 + (\lambda(v^2 - u^2)^2 = \lambda^2(4u^2v^2 + v^4 + u^4 - 2u^2v^2) = \lambda^2(v^4 + u^4 + 2u^2v^2) = (\lambda(u^2 + v^2))^2$.

Conclusion : if $x, y, z \in \mathbb{Z}$,

$$x^2 + y^2 = z^2 \iff \exists \lambda \in \mathbb{Z}, \exists (u, v) \in \mathbb{Z}^2, u \wedge v = 1,$$

$$\left\{ \begin{array}{ccc} x & = & 2\lambda uv \\ y & = & \lambda(v^2 - u^2) \\ z & = & \lambda(v^2 + u^2) \end{array} \right. \quad \text{or} \quad \left\{ \begin{array}{ccc} x & = & \lambda(v^2 - u^2) \\ y & = & 2\lambda uv \\ z & = & \lambda(v^2 + u^2) \end{array} \right.$$

□

Ex. 1.24 *Prove the identities*

(a) $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \cdots + y^{n-1})$

(b) For n *odd,* $x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + \cdots + y^{n-1})$

Proof. Let R any commutative ring, and $x, y \in R$.

a) Let

$$S = \sum_{i=0}^{n} x^{n-1-i}y^i.$$

Then

$$\begin{aligned} xS &= \sum_{i=0}^{n} x^{n-i}y^i = x^n + \sum_{i=0}^{n-1} x^{n-i}y^i \\ yS &= \sum_{i=0}^{n-1} x^{n-1-i}y^{i+1} = \sum_{j=1}^{n} x^{n-j}y^j \qquad (j = i + 1) \\ &= y^n + \sum_{i=1}^{n-1} x^{n-i}y^i. \end{aligned}$$

So $xS - yS = x^n - y^n$,

$$x^n - y^n = (x - y)\sum_{i=0}^{n} x^{n-1-i}y^i = (x - y)(x^{n-1} + x^{n-2}y + \cdots + x^{n-1-i}y^i + \cdots + y^{n-1}).$$

b) If we substitute $-y$ by y, we obtain

$$x^n - (-1)^n y^n = (x + y)\sum_{i=0}^{n}(-1)^i x^{n-1-i}y^i.$$

If n is odd,

$$x^n + y^n = (x + y)\sum_{i=0}^{n}(-1)^i x^{n-1-i}y^i = (x + y)(x^{n-1} - x^{n-2}y + \cdots + (-1)^i x^{n-1-i}y^i + \cdots + y^{n-1}).$$

□

Ex. 1.25 *If $a^n - 1$ is a prime, show that $a = 2$ and that n is a prime. Primes of the form $2^p - 1$ are called Mersenne primes. For example, $2^3 - 1 = 7$ and $2^5 - 1 = 31$. It is not known if there are infinitely many Mersenne primes.*

Proof. Suppose $n > 1, a \geq 0$, and $a^n - 1$ is a prime. As $0^n - 1 = -1, 1^n - 1 = 0$ are not primes, $a \geq 2$.

As $(a^n - 1) = (a-1)(a^{n-1} + \cdots + a^i + \cdots + 1)$, $a - 1$ is a factor of the prime $a^n - 1$, so $a - 1 = 1$ or $a - 1 = a^n - 1$.

As $a \geq 2$, and $n > 1$, $a = a^n$ is impossible, so $a = 2$.

If $n \geq 2$ wasn't prime, then $n = uv, 1 < u < n, 1 < v < n$, and

$$2^n - 1 = 2^{uv} - 1 = (2^u - 1)(2^{u(v-1)} + \cdots + 2^{ui} + \cdots + 1).$$

with $1 = 2^1 - 1 < 2^u - 1 < 2^n - 1$. $2^n - 1$ has a non trivial factor : this is impossible, so n is a prime.

Conclusion : if $a^n - 1$ $(a \geq 0, n > 1)$ is a prime, then $a = 2$ and n is a prime. $\square$

Ex. 1.26 *If $a^n + 1$ is a prime, show that a is even and that n is a power of 2. Primes of the form $2^{2^t} + 1$ are called Fermat primes. For example, $2^{2^1} + 1 = 5$ and $2^{2^2} + 1 = 17$. It is not known if there are infinitely many Fermat primes.*

Proof. If $a = 1, a^n + 1$ is a prime. Suppose $a > 1$, and $n > 1$. If a was odd, $a^n + 1 > 2$ is even, so is not a prime. Consequently, if $a^n + 1$ is prime, $a > 1$, then a is even.

Write $n = 2^t u$, where u is odd.

If $u > 1$, then, from Ex. 24(b), we obtain

$$a^n + 1 = a^{2^t u} + 1 = (a^{2^t} + 1)\sum_{i=0}^{u-1}(-1)^i a^{i2^t}.$$

So $1 < a^{2^t} + 1 < a^n + 1$, and $a^{2^t} + 1$ is a non trivial factor of $a^n + 1$, in contradiction with the hypothesis.

Conclusion : if $a^n + 1$ is a prime $(a > 1, n > 1)$, a is even and n is a power of 2. $\square$

Ex. 1.27 *For all odd n show that $8 \mid n^2 - 1$. If $3 \nmid n$, show that $6 \mid n^2 - 1$.*

Proof. As n is odd, write $n = 2k + 1, n \in \mathbb{Z}$. Then

$$n^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k = 4k(k+1).$$

As k or $k + 1$ is even, $8 \mid n^2 - 1$.

$(n-1)n(n+1) = n(n^2 - 1)$, product of three consecutive numbers, is a multiple of 3.

As $3 \nmid n$, and 3 is a prime, $3 \wedge n = 1$, so $3 \mid n^2 - 1$.

$$3 \nmid n \Rightarrow 3 \mid n^2 - 1.$$

(This is also a consequence of Fermat' Little Theorem.)

As n is odd, $n^2 - 1$ is even. $3 \mid n^2 - 1, 2 \mid n^2 - 1$ and $2 \wedge 3 = 1$, so $6 \mid n^2 - 1$. $\square$

Ex. 1.28 *For all n show that $30 \mid n^5 - n$ and that $42 \mid n^7 - n$.*

Proof. If we want to avoid Fermat's Little Theorem (Prop. 3.3.2. Corollary 2 P. 33), note that

$$\begin{aligned}(n-2)(n-2)n(n+1)(n+2) &= n(n^2-1)(n^2-4)\\ &= n^5 - 5n^2 + 4n\\ &= n^5 - n + 5(-n^2+n)\end{aligned}$$

As the product of 5 consecutive numbers is divisible by 5,

$$5 \mid n^5 - n.$$

Moreover,

$$\begin{aligned}&2 \mid (n-1)(n+1) = n^2 - 1 \mid n^4 - 1 \mid n^5 - n\\ &3 \mid (n-1)n(n+1) = n(n^2-1) \mid n(n^4-1) = n^5 - n\end{aligned}$$

As $2, 3, 5$ are distinct primes, $2 \times 3 \times 5 = 30 \mid n^5 - n$.

Similarly,

$$\begin{aligned}(n-3)(n-2)(n-1)n(n+1)(n+2)(n+3) &= n(n^2-1)(n^2-4)(n^2-9)\\ &= n(n^4 - 5n^2 + 4)(n^2 - 9)\\ &= n^7 - 14n^5 + 49n^3 - 36n\\ &= n^7 - n + 7(-2n^5 + 7n^3 - 5n)\end{aligned}$$

As the product of 7 consecutive numbers is divisible by 7,

$$7 \mid n^7 - n.$$

Moreover

$$\begin{aligned}&2 \mid (n-1)(n+1) = n^2 - 1 \mid n^6 - 1 \mid n^7 - n\\ &3 \mid (n-1)n(n+1) = n(n^2-1) \mid n(n^6-1) = n^7 - n\end{aligned}$$

As $2, 3, 7$ are distinct primes $2 \times 3 \times 7 = 42 \mid n^7 - n$. $\square$

Ex. 1.29 *Suppose that $a, b, c, d \in \mathbb{Z}$ and that $(a, b) = (c, d) = 1$.*
If $(a/b) + (c/d) =$ an integer, show that $b = \pm d$.

Proof. If $\frac{a}{b} + \frac{c}{d} = n \in \mathbb{Z}$ $\quad (a \wedge b = c \wedge d = 1)$, then $ad + bc = nbd$, so $d \mid bc, d \wedge c = 1$, which implies $d \mid b$. Similarly $b \mid d$. Then $d = \pm b$. $\square$

Ex. 1.30 *Prove that $H_n = \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ is not an integer.*

Proof. Let s such that $2^s \le n < 2^{s+1}$ $(s = \left\lfloor \frac{\ln n}{\ln 2} \right\rfloor \ge 1)$.

$$H_n = \frac{1}{2} + \cdots + \frac{1}{n} = \frac{\sum_{i=2}^n a_i}{n!}, \qquad \text{where } a_i = \frac{n!}{i} \in \mathbb{Z}.$$

Let $k = \mathrm{ord}_2(n!)$. We will show that $\mathrm{ord}_s(a_i)$ is minimal for $i_0 = 2^s$, where $\mathrm{ord}_2(a_{i_0}) = k - s$, and that this minimum is reached only for this index i_0.

Indeed, each i such that $2 \le i \le n$ can be written with the form $i = 2^t q, 2 \nmid q$. Then $i = 2^t q \le n < 2^{s+1}$, so $2^t < 2^{s+1}, t < s+1, t \le s$, which proves

$$\mathrm{ord}_2(a_i) = k - t \ge k - s = \mathrm{ord}_2(a_{i_0}).$$

Moreover, if $\mathrm{ord}_2(a_i) = \mathrm{ord}_2(a_{i_0})$, then $k - t = k - s$, so $s = t$.

$i = 2^s q, 2 \nmid q$. If $q > 1$, then $i \ge 2^{s+1} > n$: it's impossible. So $q = 1$ and $i = 2^s = i_0$.

Using Ex 1.21, we see that

$$\mathrm{ord}_2\left(\sum_{i=2}^{n} a_i\right) = \mathrm{ord}_2(a_{i_0}) = k - s < k = \mathrm{ord}_2(n!).$$

So

$$H_n = \frac{2^{k-s}Q}{2^k R} = \frac{Q}{2^s R},$$

where Q, R are odd integers. H_n is a quotient of an odd integer by an even integer : H_n is never an integer. □

Ex. 1.31 *Show that 2 is divisible by $(1+i)^2$ in $\mathbb{Z}[i]$.*

Proof. $(1+i)^2 = 1 + 2i - 1 = 2i$, so $2 = -i(1+i)^2$ is divisible by $(1+i)^2$. (As i is an unit, 2 and $(1+i)^2$ are associate.) □

Ex. 1.32 *For $\alpha = a + bi \in \mathbb{Z}[i]$ we defined $\lambda(\alpha) = a^2 + b^2$. From the properties of λ deduce the identity $(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$.*

Proof. For all complex numbers α, β, $|\alpha\beta| = |\alpha||\beta|$, so

$$\lambda(\alpha\beta) = \lambda(\alpha)\lambda(\beta).$$

If $\alpha = a + bi \in \mathbb{Z}[i), \beta = c + di \in \mathbb{Z}[i]$, then $\alpha\beta = (ac - bd) + (ad + bc)i$, so

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2.$$

□

Ex. 1.33 *Show that $\alpha \in \mathbb{Z}[i]$ is a unit iff $\lambda(\alpha) = 1$. Deduce that 1, -1, i, and - i are the only units in $\mathbb{Z}[i]$.*

Proof. Let $\alpha = a + bi \in \mathbb{Z}[i]$.

- If $\lambda(\alpha) = 1$, then $\alpha\overline{\alpha} = 1$, where $\overline{\alpha} = a - bi \in \mathbb{Z}[i]$, so α is an unit.
- Reciprocally, if α is an unit, there exists $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = 1$, then $\lambda(\alpha)\lambda(\beta) = 1$, where $\lambda(\alpha), \lambda(\beta)$ are positive integers, hence $\lambda(\alpha) = 1$.

So $\alpha = a + ib$ is an unit of $\mathbb{Z}[i]$ if and only if $a^2 + b^2 = 1$. In this case, $|a|^2 \le 1$, $a \in \{0, 1, -1\}$. If $a = 0, b = \pm 1$, and if $a = \pm 1, b = 0$, so the only units of $\mathbb{Z}[i]$ are $1, i, -1, -i$. □

Ex. 1.34 *Show that 3 is divisible by $(1-\omega)^2$ in $\mathbb{Z}[\omega]$.*

Proof. As $\omega^3 = 1, \overline{\omega} = \omega^2$, and $1+\omega+\omega^2 = 0$,
$|1-\omega|^2 = (1-\omega)(1-\omega^2) = 1+\omega^3-\omega-\omega^2 = 3$, so

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

Consequently,

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

3 is divisible by $(1-\omega)^2$ in $\mathbb{Z}[\omega]$ (as $-\omega^2$ is an unit, 3 and $(1-\omega)^2$ are associated. 3 is not irreducible in $\mathbb{Z}[\omega]$). $\square$

Ex. 1.35 *For $\alpha = a+b\omega \in \mathbb{Z}[\omega]$ we defined $\lambda(\alpha) = a^2-ab+b^2$. Show that α is a unit iff $\lambda(\alpha) = 1$. Deduce that $1, -1, \omega, -\omega, \omega^2, and -\omega^2$ are the only units in $\mathbb{Z}[\omega]$.*

Proof. If $\alpha = a+b\omega \in \mathbb{Z}[\omega]$, using $1+\omega+\omega^2 = 0$ and $\overline{\omega} = \omega^2$, we obtain

$$\begin{aligned}\alpha\overline{\alpha} &= (a+b\omega)(a+b\omega^2)\\ &= a^2+b^2+ab(\omega+\omega^2)\\ &= a^2+b^2-ab\\ &= \lambda(\alpha)\end{aligned}$$

Consequently, λ is a multiplicative function.

• If $\lambda(\alpha) = 1$, then $\alpha\overline{\alpha} = 1$, where $\overline{\alpha} = a+b\omega^2 = (a-b)-b\omega \in \mathbb{Z}[\omega]$, so α is an unit.

• Reciprocally, if α is an unit, there exists $\beta \in \mathbb{Z}[\omega]$ such that $\alpha\beta = 1$, then $\lambda(\alpha)\lambda(\beta) = 1$, where $\lambda(\alpha), \lambda(\beta)$ are positive integers, so $\lambda(\alpha) = 1$.

$$\begin{aligned}\lambda(\alpha) = 1 &\iff a^2-ab+b^2 = 1\\ &\iff (2a-b)^2+3b^2 = 4\end{aligned}$$

$3b^2 \leq 4$, so $b = 0$ or $b = \pm 1$.

If $b = 0$, then $a = \pm 1$, $\alpha = 1$ or $\alpha = -1$

If $b = 1$, then $(2a-1)^2 = 1, 2a-1 = \pm 1$: $a = 0$ or $a = 1$, $\alpha = \omega$ or $\alpha = 1+\omega = -\omega^2$.

If $b = -1$, then $(2a+1)^2 = 1, 2a+1 = \pm 1$: $a = 0$ or $a = -1$, $\alpha = -\omega$ or $\alpha = -1-\omega = \omega^2$.

So

$$\lambda(\alpha) = 1 \iff \alpha \in \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}.$$

The set of units of $\mathbb{Z}[\omega]$ is the group of the roots of x^6-1. $\square$

Ex. 1.36 *Define $\mathbb{Z}[\sqrt{-2}]$ as the set of all complex numbers of the form $a+b\sqrt{-2}$, where $a, b \in \mathbb{Z}$. Show that $\mathbb{Z}[\sqrt{-2}]$ is a ring. Define $\lambda(\alpha) = a^2+2b^2$ for $\alpha = a+b\sqrt{-2}$. Use λ to show that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.*

Proof. Note $\sqrt{-2} = i\sqrt{2}$, and $A = \mathbb{Z}[\sqrt{-2}]$.

Let $\alpha = a + b\sqrt{-2}, \beta = c + d\sqrt{-2} \in A$:

- $1 = 1 + 0\sqrt{-2} \in A$.
- $\alpha - \beta = (a + b\sqrt{-2}) - (c + d\sqrt{-2}) = (a - c) + (b - d)\sqrt{-2} \in A$.
- $\alpha\beta = (a + b\sqrt{-2})(c + d\sqrt{-2}) = (ac - 2bd) + (ad + bc)\sqrt{-2} \in A$.

So A is a subring of $(\mathbb{C}, +, \times)$: $\mathbb{Z}[\sqrt{-2}]$ is a ring.

Let $z = a + ib\sqrt{-2}$ any complex number. Let $a_0, b_0 \in \mathbb{Z}$ such that $|a - a_0| \leq 1/2, |b - b_0| \leq 1/2$ (it suffice to take for a_0 the nearest integer of a : $a_0 = \lfloor a + \frac{1}{2} \rfloor$). Let $z_0 = a_0 + ib_0\sqrt{-2}$.

As $\lambda(z) = z\overline{z} = a^2 + 2b^2$, then

$$\lambda(z - z_0) = (a - a_0)^2 + 2(b - b_0)^2 \leq \frac{1}{4} + 2 \times \frac{1}{4} = \frac{3}{4} < 1.$$

Conclusion : for any $z \in \mathbb{C}$, there exists $z_0 \in A$ such that $\lambda(z - z_0) < 1$.

Let $(z_1, z_2) \in A \times A, z_2 \neq 0$. We apply the preeceeding result to the complex z_1/z_2 : there exists $q \in A$ such that $\left|\frac{z_1}{z_2} - q\right| \leq 1$. Let $r = z_1 - qz_2$. Then $z_1 = qz_2 + r, \lambda(r) < \lambda(z_2)$.

So $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain. $\square$

Ex. 1.37 *Show that the only units in $\mathbb{Z}[\sqrt{-2}]$ are 1 and -1.*

Proof. As in Ex. 35, we prove that $\alpha = a + b\sqrt{-2}$ is an unit if and only if $\lambda(\alpha) = 1$, i.e. $a^2 + 2b^2 = 1$. As $2b^2 \leq 1, b = 0$, and $a^2 = 1$. So the only units are 1 and -1. $\square$

Ex. 1.38 *Suppose that $\pi \in \mathbb{Z}[i]$ and that $\lambda(\pi) = p$ is a prime in $\mathbb{Z}$. Show that π is a prime in $\mathbb{Z}[i]$. Show that the corresponding result holds in $\mathbb{Z}[\omega]$ and $\mathbb{Z}[\sqrt{-2}]$.*

Proof. If $\pi = \alpha\beta$, where $\alpha, \beta \in \mathbb{Z}[i]$, then $p = \lambda(\pi) = \lambda(\alpha)\lambda(\beta)$. As p is a prime in $\mathbb{Z}$, and $\lambda(\alpha) \geq 0, , \lambda(\beta) \geq 0$, $\lambda(\alpha) = 1$ or $\lambda(\beta) = 1$, so (Ex.1.33) α or β is an unit. Consequently, π is irreducible in $\mathbb{Z}[i]$. As $\mathbb{Z}[i]$ is a PID, π is a prime in $\mathbb{Z}[i]$ (Prop. 1.3.2 Corollary 2).

As $\mathbb{Z}[\omega]$ and $\mathbb{Z}[\sqrt{-2}]$ are Euclidean domains, the same result is true in these principal ideals domains. $\square$

Ex. 1.39 *Show that in any integral domain a prime element is irreducible.*

Proof. Let R an integral domain, and π a prime in R.

If $\pi = \alpha\beta,\ \alpha, \beta \in R$, a fortiori π divides $\alpha\beta$. As π is a prime, π divides α or β, say α, so there exists $\xi \in R$ such that $\alpha = \xi\pi$, so $\pi = \xi\pi\beta, \pi(1 - \xi\beta) = 0$. As A is an integral domain, and $\pi \neq 0$ by definition, $1 = \xi\beta$, so β is an unit. If $\pi = \alpha\beta$, α or β is an unit, so π is irreducible. $\square$

2 Chapter 2

Ex 2.1 *Show that $k[x]$, with k a finite field, has infinitely many irreducible polynomials.*

Proof. Suppose that the set S of irreducible polynomials is finite : $S = \{P_1, P_2, \ldots, P_n\}$.

Let $Q = P_1P_2 \cdots P_n + 1$. As S contains the polynomials $x - a, a \in k$, $\deg(Q) \geq q = |k| > 1$. Thus Q is divisible by an irreducible polynomial. As S contains all the irreducible polynomials, there exists $i, 1 \leq i \leq n$, such that $P_i \mid Q = P_1P_2\cdots P_n + 1$, so $P_i \mid 1$, and P_i is an unit, in contradiction with the irreducibility of P_i.

Conclusion : $k[x]$ has infinitely many irreducible polynomials. As each polynomial has only a finite number of associates, there exists infinitely many monic irreducible polynomials. □

Ex. 2.2. *Let $p_1, p_2, \ldots, p_t \in \mathbb{Z}$ be primes and consider the set of all rational numbers $r = a/b,\ a, b \in \mathbb{Z}$, such that $\mathrm{ord}_{p_i} a \geq \mathrm{ord}_{p_i} b$ for $i = 1, 2, \ldots, t$. Show that this set is a ring and that up to taking associates $p_1, p_2, \ldots, p_t$ are the only primes.*

Proof. Let R the set of such rationals. Simplifying these fractions, we obtain

$$r \in R \iff \exists p \in \mathbb{Z}, \exists q \in \mathbb{Z} \setminus \{0\},\ r = \frac{p}{q},\ q \wedge p_1p_2\cdots p_t = 1.$$

• $1 = 1/1 \in R$.

• if $r, r' \in R$, $r = p/q, r' = p'/q'$, with $q \wedge p_1p_2\cdots p_t = 1, q' \wedge p_1p_2\cdots p_t = 1$. then $qq' \wedge p_1p_2\cdots p_t = 1$, and $r - r' = \frac{pq'-qp'}{qq'}$, $rr' = \frac{pp'}{qq'}$, so $r - r', rr' \in R$.

Thus R is a subring of $\mathbb{Q}$.

If $r = a/b \in R$ is an unit of R, then $b/a \in R$, so $\mathrm{ord}_{p_i} a = \mathrm{ord}_{p_i}(b),\ i = 1, \ldots, t$. After simplification, $r = p/q$, with $p \wedge p_1\cdots p_t = 1, q \wedge p_1\cdots p_t = 1$, and such rationals are all units.

$p_i, 1 \leq i \leq t$, is a prime : if $p_i \mid rs$ in R, where $r = a/b, s = c/d \in R$, then there exists $u = e/f \in R$ such that $rs = p_iu$, with b, d, e relatively prime with $p_1, \ldots, p_t$. Then $acf = p_ibde$. As $p_i \wedge f = 1$, p_i divides a or c in $\mathbb{Z}$, so p_i divides r or s in R.

If $r = a/b \in R$, with $b \wedge p_1\cdots p_r = 1$, $a = p_1^{k_1}\cdots p_t^{k_t}v, v \in \mathbb{Z}, k_i \geq 0, i = 1, \ldots, t$. So $r = up_1^{k_1}\cdots p_t^{k_t}$, where $u = v/b$ is an unit.

Let π be any prime in R. As any element in R, $\pi = up_1^{k_1}\cdots p_t^{k_t}, k_i \geq 0, u = a/b$ an unit. $u^{-1}\pi = p_1^{k_1}\cdots p_t^{k_t}$, so $\pi \mid p_1^{k_1}\cdots p_t^{k_t}$ (in R). As π is a prime in R, $\pi \mid p_i$ for an index $i = 1, \ldots, t$. Moreover $p_i \mid p$, so p_i and π are associate.

Conclusion: the primes in R are the associates of $p_1, \ldots, p_t$. □

Ex. 2.3 *Use the formula for $\phi(n)$ to give a proof that there are infinitely many primes. [Hint: If $p_1, p_2, \ldots, p_t$ were all the primes, then $\phi(n) = 1$, where $n = p_1p_1\cdots p_t$.]*

Proof. Let $\{p_1, \cdots, p_t\}$ the finite set of primes,with $p_1 < p_2 < \cdots < p_t$, and $n = p_1\cdots p_t$. By définition, $\phi(n)$ is the number of integers $k, 1 \leq k \leq n$, such that $k \wedge n = 1$. From the existence of decomposition in primes, if $k \geq 1$, $k = p_1^{k_1}\cdots p_t^{k_t}$, where $k_i \geq 0, i = 1, \ldots, t$. So $k \wedge n = 1$ if and only if $k = 1$. Thus $\phi(n) = 1$ The formula for $\phi(n)$ gives $\phi(n) = (p_1 - 1)\cdots(p_t - 1) = 1$. As $p_i \geq 2$, this equation implies that $p_1 = p_2 = \cdots = p_t = 2$, so $t = 1$, and the only prime number is 2. But 3 is also a prime number : this is a contradiction.

Conclusion : there are infinitely many prime numbers. □

Ex. 2.4 *If a is a nonzero integer, then for $n > m$ show that $(a^{2^n} + 1, a^{2^m} + 1) = 1$ or 2 depending on whether a is odd or even.*

Proof. Let $d = a^{2^n} + 1 \wedge a^{2^m} + 1$. Then $d \mid a^{2^n} + 1, d \mid a^{2^m} + 1$. So

$$a^{2^n} \equiv -1 \pmod{d}$$
$$a^{2^m} \equiv -1 \pmod{d}$$

As $n > m$, 2^{n-m} is even, so

$$-1 \equiv a^{2^n} = \left(a^{2^m}\right)^{2^{n-m}} \equiv (-1)^{2^{n-m}} \equiv 1 \pmod{d}.$$

$-1 \equiv 1 \pmod{d}$, then $d \mid 2$ ($d \geq 0$). Thus $d = 1$ or $d = 2$.

If a is even, $a^{2^n} + 1$ is odd, so $d = 1$.

If a is odd, both $a^{2^n} + 1, a^{2^m} + 1$ are even, so $d = 2$. □

Ex. 2.5 *Use the result of Ex. 2.4 to show that there are infinitely many primes. (This proof is due to G.Polya.)*

Proof. Let $F_n = 2^{2^n} + 1, n \in \mathbb{N}$. We know from Ex. 2.4 that $n \neq m \Rightarrow F_n \wedge F_m = 1$. Define p_n as the least prime divisor of F_n. If $n \neq m, F_n \wedge F_m = 1$, so $p_n \neq p_m$. The application $\varphi : \mathbb{N} \to \mathbb{N}, n \mapsto p_n$ is injective (one to one), so $\varphi(\mathbb{N})$ is an infinite set of prime numbers. □

Ex. 2.6 *For a rational number r let $\lfloor r \rfloor$ be the largest integer less than or equal to r, e.g., $\lfloor \frac{1}{2} \rfloor = 0$, $\lfloor 2 \rfloor = 2$, and $\lfloor 3 + \frac{1}{3} \rfloor = 3$. Prove* $\operatorname{ord}_p n! = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor \cdots$.

Proof. The number N_k of multiples m of p^k which are not multiple of p^{k+1}, where $1 \leq m \leq n$, is

$$N_k = \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor.$$

Each of these numbers brings the contribution k to the sum $\operatorname{ord}_p n! = \sum\limits_{k=1}^{n} \operatorname{ord}_p k$. Thus

$$\begin{aligned}
\operatorname{ord}_p n! &= \sum_{k \geq 1} k \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) \\
&= \sum_{k \geq 1} k \left\lfloor \frac{n}{p^k} \right\rfloor - \sum_{k \geq 1} k \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \\
&= \sum_{k \geq 1} k \left\lfloor \frac{n}{p^k} \right\rfloor - \sum_{k \geq 2} (k-1) \left\lfloor \frac{n}{p^k} \right\rfloor \\
&= \left\lfloor \frac{n}{p} \right\rfloor + \sum_{k \geq 2} \left\lfloor \frac{n}{p^k} \right\rfloor \\
&= \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor
\end{aligned}$$

Note that $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$ if $p^k > n$, so this sum is finite. □

Ex. 2.7 *Deduce from Ex. 2.6 that* $\operatorname{ord}_p n! \leq n/(p-1)$ *and that* $\sqrt[n]{n!} \leq \prod_{p \leq n} p^{1/(p-1)}$.

(The original statement $\prod_{p \mid n} p^{1/(p-1)}$ was modified.)

Proof.

$$\operatorname{ord}_p n! = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor \leq \sum_{k \geq 1} \frac{n}{p^k} = \frac{n}{p} \frac{1}{1 - \frac{1}{p}} = \frac{n}{p-1}$$

The decomposition of $n!$ in prime factors is
$n! = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where $\alpha_i = \mathrm{ord}_{p_i} n! \leq \frac{n}{p_i - 1}$, and $p_i \leq n, \ i = 1, 2, \cdots, k$.
Then

$$\begin{aligned} n! &\leq p_1^{\frac{n}{p_1-1}} p_2^{\frac{n}{p_2-1}} \cdots p_k^{\frac{n}{p_n-1}} \\ \sqrt[n]{n!} &\leq p_1^{\frac{1}{p_1-1}} p_2^{\frac{1}{p_2-1}} \cdots p_k^{\frac{1}{p_n-1}} \\ &\leq \prod_{p \leq n} p^{\frac{1}{p-1}} \end{aligned}$$

(the values of p in this product describe all prime numbers $p \leq n$.) $\square$

Ex. 2.8 *Use Exercise 7 to show that there are infinitely many primes.*

Proof. If the set $\mathbb{P}$ of prime numbers was finite, we obtain from Ex.2.7, for all $n \geq 2$:

$$\sqrt[n]{n!} \leq C = \prod_{p \in \mathbb{P}} p^{\frac{1}{p-1}},$$

where C is an absolute constant.

Yet $\lim_{n \to \infty} \sqrt[n]{n!} = +\infty$. Indeed

$$\ln(\sqrt[n]{n!}) = \frac{1}{n}(\ln 1 + \ln 2 + \cdots + \ln n)$$

As ln is an increasing fonction,

$$\int_{i-1}^{i} \ln t \,\mathrm{d}t \leq \ln i, \ i = 2, 3, \ldots, n$$

So

$$\int_1^n \ln t \,\mathrm{d}t = \sum_{i=2}^{n} \int_{i-1}^{i} \ln t \,\mathrm{d}t \leq \sum_{i=2}^{n} \ln i = \sum_{i=1}^{n} \ln i$$

Thus

$$\ln(\sqrt[n]{n!}) \geq \frac{1}{n} \int_1^n \ln t \,\mathrm{d}t \ = \frac{1}{n}(n \ln n - n + 1) = \ln n - 1 + \frac{1}{n}$$

As $\lim_{n \to \infty} \ln n - 1 + \frac{1}{n} = +\infty$, $\lim_{n \to \infty} \ln(\sqrt[n]{n!}) = +\infty$, so $\lim_{n \to \infty} \sqrt[n]{n!} = +\infty$.

So there exists n such that $\sqrt[n]{n!} \geq C$: this is a contradiction. $\mathbb{P}$ is an infinite set. $\square$

Ex. 2.9 *A function on the integers is said to be multiplicative if $f(ab) = f(a)f(b)$. whenever $(a, b) = 1$. Show that a multiplicative function is completely determined by its value on prime powers.*

Proof. Let the decomposition of n in prime factors be $n = p_1^{k_1} \cdots p_t^{k_t}, p_1 < \cdots < p_t$. As $p_i^{k_i} \wedge p_j^{k_j} = 1$ for $i \neq j, \ i, j = 1, \ldots, t$,

$$f(n) = f(p_1^{k_1} \cdots p_t^{k_t}) = f(p_1^{k_1}) \cdots f(p_t^{k_t})$$

(by induction on the number of prime factors.)

So $f(n)$ is completely determined by its value on prime powers. $\square$

Ex. 2.10 *If $f(n)$ is a multiplicative function, show that the function $g(n) = \sum_{d|n} f(d)$ is also multiplicative.*

Proof. If $n \wedge m = 1$,

$$\begin{aligned} g(nm) &= \sum_{\delta | nm} f(\delta) \\ &= \sum_{d|n, d'|m} f(dd') \end{aligned}$$

Actually, if $d \mid n, d' \mid m$, so $\delta = dd' \mid nm$, and reciprocally, if $\delta \mid nm$, as $n \wedge m = 1$, there exist d, d' such that $d \mid n, d' \mid m$, and $\delta = dd'$.

If $d \mid n, d' \mid m$, with $n \wedge m = 1$, then $d \wedge d' = 1$, so

$$\begin{aligned} g(nm) &= \sum_{d|n} \sum_{d'|m} f(d) f(d') \\ &= \sum_{d|n} f(d) \sum_{d'|m} f(d') \\ &= g(n) g(m) \end{aligned}$$

g is a multiplicative function. $\square$

Ex. 2.11 *Show that $\phi(n) = n \sum_{d|n} \mu(d)/d$ by first proving that $\mu(d)/d$ is multiplicative and then using Ex. 2.9 and 2.10.*

Proof. Let's verify that μ is a multiplicative function.

If $n \wedge m = 1$, then $n = p_1^{a_1} \cdots p_l^{a_l}, m = q_1^{b_1} \cdots q_r^{b_r}$, where $p_1, \ldots, p_l, q_1, \ldots q_r$ are distinct primes. Then the decomposition in prime factors of nm is $nm = p_1^{a_1} \cdots p_l^{a_l} q_1^{b_1} \cdots q_r^{b_r}$. If one of the a_i or one of the b_j is greater than 1, then $\mu(nm) = 0 = \mu(n)\mu(m)$. Otherwise, $n = p_1 \cdots p_l, m = q_1 \cdots q_r, nm = p_1 \cdots p_l q_1 \cdots q_r$, and $\mu(nm) = (-1)^{l+r} = (-1)^l (-1)^r = \mu(n)\mu(m)$. So

$$\frac{\mu(nm)}{nm} = \frac{\mu(n)}{n} \frac{\mu(m)}{m}.$$

that is, $n \mapsto \frac{\mu(n)}{n}$ is a multiplicative function.

From Ex.2.10, $n \mapsto \sum_{d|n} \frac{\mu(d)}{d}$ is also a multiplicative function, and so is ψ, where ψ is defined by

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

To verify the equality $\phi = \psi$, it is sufficient from Ex. 2.9 to verify $\phi(p^k) = \psi(p^k)$ for all prime powers $p^k, k \geq 1$ ($\phi(1) = \psi(1) = 1$).

$$\begin{aligned} \psi(p^k) &= p^k \sum_{d|p^k} \frac{\mu(p^k)}{p^k} \\ &= p^k \left(\frac{\mu(1)}{1} + \frac{\mu(p)}{p} \right) \end{aligned}$$

(The other terms are null.)

So

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

Thus $\phi = \psi$: for all $n \geq 1$,

$$\phi(n) = n\sum_{d|n} \frac{\mu(d)}{d}.$$

$\square$

Ex. 2.12 *Find formulas for* $\sum_{d|n} \mu(d)\phi(d)$, $\sum_{d|n} \mu(d)^2\phi(d)^2$, *and* $\sum_{d|n} \mu(d)/\phi(d)$.

Proof. As μ, ϕ are multiplicative, so are $\mu\phi, \mu^2\phi^2, \mu/\phi$. We deduce from Ex. 2.10 that the three following fonctions F, G, H are multiplicative, defined by

$$F(n) = \sum_{d|n} \mu(d)\phi(d), G(n) = \sum_{d|n} \mu(d)^2\phi(d)^2, H(n) = \sum_{d|n} \mu(d)/\phi(d),$$

so it is sufficient to compute their values on prime powers $p^k, k \geq 1$.

$$\begin{aligned} F(p^k) &= \sum_{i=0}^{k} \mu(p^i)\phi(p^i) \\ &= \phi(1) - \phi(p) = 1 - (p-1) = 2 - p \end{aligned}$$

So $F(n) = \sum_{p|n}(2-p)$.

Similarly,

$$\begin{aligned} G(p^k) &= \sum_{i=0}^{k} \mu(p^i)^2\phi(p^i)^2 \\ &= \phi(1)^2 + \phi(p)^2 = 1 + (p-1)^2 = p^2 - 2p + 2 \end{aligned}$$

$$\begin{aligned} H(p^k) &= \sum_{i=0}^{k} \mu(p^i)/\phi(p^i) \\ &= 1/\phi(1) - 1/\phi(p) = 1 - 1/(p-1) = (p-2)/(p-1) \end{aligned}$$

$\square$

Ex. 2.13 *Let* $\sigma_k(n) = \sum_{d|n} d^k$. *Show that* $\sigma_k(n)$ *is multiplicative and find a formula for it.*

Proof. As $n \mapsto n^k$ is multiplicative, then so is σ_k (Ex. 2.10).

• Suppose $k \neq 0$.

If $n = p^\alpha$ is a prime power ($\alpha \geq 1$),

$$\begin{aligned} \sigma_k(p^\alpha) &= \sum_{i=0}^{\alpha} p^{ik} \\ &= \frac{p^{(\alpha+1)k} - 1}{p^k - 1} \end{aligned}$$

- if $k=0$, $\sigma_0(n)$ is the number of divisors of n.

$$\begin{aligned}\sigma_0(p^\alpha) &= \sum_{i=0}^{\alpha} 1\\ &= \alpha+1\end{aligned}$$

Conclusion : if $n = p_1^{\alpha_1}\cdots p_t^{\alpha_t}$ is the decomposition of n in prime factors, then

$$\begin{aligned}\sigma_0(n) &= (\alpha_1+1)\cdots(\alpha_t+1),\\ \sigma_k(n) &= \prod_{i=0}^{t} \frac{p_i^{(\alpha_i+1)k}-1}{p_i^k-1} \ (k\neq 0).\end{aligned}$$

□

Ex. 2.14 *If $f(n)$ is multiplicative, show that $h(n)=\sum_{d\mid n}\mu(n/d)f(d)$ is also multiplicative.*

Proof. We show first that the Dirichlet product $f\circ g$ of two multiplicative functions f,g is multiplicative. Suppose that $n\wedge m=1$. If $d\mid n, d'\mid m$, so $\delta=dd'\mid nm$, and reciprocally, if $\delta\mid nm$, as $n\wedge m=1$, there exist d,d' such that $d\mid n, d'\mid m$, and $\delta=dd'$. Thus

$$\begin{aligned}(f\circ g)(nm) &= \sum_{\delta\mid nm} f(\delta)g\left(\frac{m}{\delta}\right)\\ &= \sum_{d\mid n, d'\mid m} f(dd')g\left(\frac{nm}{dd'}\right)\\ &= \sum_{d\mid n}\sum_{d'\mid m} f(d)f(d')g\left(\frac{n}{d}\right)g\left(\frac{m}{d'}\right)\\ &= \sum_{d\mid n} f(d)g\left(\frac{n}{d}\right)\sum_{d'\mid m} f(d')g\left(\frac{m}{d'}\right)\\ &= (f\circ g)(n)(f\circ g)(m)\end{aligned}$$

Applying this result with $g=\mu$, we obtain that $n\mapsto h(n)=\sum_{d\mid n}\mu(n/d)f(d)$ is multiplicative, if f is multiplicative. □

Ex. 2.15 *Show that*

(a) $\sum_{d\mid n}\mu(n/d)\nu(d)=1$ *for all* n.

(b) $\sum_{d\mid n}\mu(n/d)\sigma(d)=n$ *for all* n.

Proof. Here $\nu=\sigma_0, \sigma=\sigma_1$.

(a) From the Möbius Inversion Theorem, as $\nu(n)=\sum_{d\mid n}1=\sum_{d\mid n}I(d)$, where $I(n)=1$ for all $n\geq 1$,

$$1 = I(n) = \sum_{d\mid n}\mu(n/d)\nu(d).$$

(b) From the same theorem, as $\sigma(n) = \sum_{d|n} d = \sum_{d|n} \mathrm{Id}(d)$, where $\mathrm{Id}(n) = n$ for all $n \geq 1$,

$$n = \mathrm{Id}(n) = \sum_{d|n} \mu(n/d)\sigma(d).$$

$\square$

Ex. 2.16 *Show that $\nu(n)$ is odd iff n is a square.*

Proof. • If $n = a^2$ is a square, where $a = p_1^{k_1} \cdots p_t^{k_t}$, then $\nu(n) = (2k_1 + 1) \cdots (2k_t + 1)$ is odd.

• Reciprocally, if $n = q_1^{l_1} \cdots q_r^{l_r}$ is odd, then $(l_1 + 1) \cdots (l_r + 1)$ is odd. So each $l_i + 1$ is odd, and then l_i is even, for $i = 1, 2, \ldots, r$: n is a square. $\square$

Ex. 2.17 *Show that $\sigma(n)$ is odd iff n is a square or twice a square.*

Proof. • Note that for all $r \geq 0$, $\sigma(2^r) = 1 + 2 + 2^2 + \cdots + 2^r = 2^{r+1} - 1$ is always odd.
If $p \neq 2$, $\sigma(p^{2k}) = 1 + p + p^2 + \cdots + p^{2k}$ is a sum of $2k + 1$ odd numbers, so is odd.
So if $n = a^2$, or $n = 2a^2, a \in \mathbb{Z}$, $\sigma(n)$ is odd.

• Reciprocally, suppose that $\sigma(n)$ is odd, where $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$, with $p_1 = 2 < p_2 < \cdots < p_t$. Then

$$\sigma(n) = (2^{k_1+1} - 1)\frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_t^{k_t+1} - 1}{p_t - 1}$$

is odd. Then each $\frac{p_i^{k_i+1}-1}{p_i-1} = 1 + p_i + \cdots + p_i^{k_i}$ $(i = 2, \cdots, t)$ is odd. As each $p_i^j, j = 0, \ldots, k_i$ is odd, the number of terms $k_i + 1$ is odd, so k_i is even $(i = 2, \ldots, t)$. Thus n is a square, or twice a square. $\square$

Ex. 2.18 *Prove that $\phi(n)\phi(m) = \phi((n, m))\phi([n, m])$.*

Proof. Let $p_1, \cdots, p_r$ the common prime factors of n and m.

$$\begin{aligned} n &= p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\lambda_1} \cdots q_s^{\lambda_s} \\ m &= p_1^{\beta_1} \cdots p_r^{\beta_r} s_1^{\mu_1} \cdots s_t^{\mu_t} \end{aligned}$$

where $\alpha_i, \beta_i, \lambda_j, \mu_k \in \mathbb{N}^*$, $1 \leq i \leq r, 1 \leq j \leq s, 1 \leq k \leq t$ (the formula $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$ is not valid if $\alpha = 0$). Then

$$\begin{aligned} n \wedge m &= p_1^{\gamma_1} \cdots p_r^{\gamma_r} \\ n \vee m &= p_1^{\delta_1} \cdots p_r^{\delta_r} q_1^{\lambda_1} \cdots q_s^{\lambda_s} s_1^{\mu_1} \cdots s_t^{\mu_t}, \end{aligned}$$

where $\gamma_i = \min(\alpha_i, \beta_i), \delta_i = \max(\alpha_i, \beta_i)$ $(\gamma_i \geq 1, \delta_i \geq 1), 1 \leq i \leq r$. Then

$$\begin{aligned} \phi(n \wedge m) &= \prod_{i=1}^{r} (p_i^{\gamma_i} - p_i^{\gamma_i - 1}) \\ \phi(n \vee m) &= \prod_{i=1}^{r} (p_i^{\delta_i} - p_i^{\delta_i - 1}) \prod_{i=1}^{s} (q_i^{\lambda_i} - q_i^{\lambda_i - 1}) \prod_{i=1}^{t} (s_i^{\mu_i} - s_i^{\mu_i - 1}) \end{aligned}$$

As $\alpha_i + \beta_i = \min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \gamma_i + \delta_i, 1 \le i \le r$, then

$$\begin{aligned}
\phi(n)\phi(m) &= \prod_{i=1}^{r}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) \prod_{i=1}^{s}(q_i^{\lambda_i} - q_i^{\lambda_i - 1}) \prod_{i=1}^{r}(p_i^{\beta_i} - p_i^{\beta_i - 1}) \prod_{i=1}^{t}(s_i^{\mu_i} - s_i^{\mu_i - 1}) \\
&= \prod_{i=1}^{r} \left[p_i^{\alpha_i + \beta_i} \left(1 - \frac{1}{p_i}\right)^2 \right] \prod_{i=1}^{s}(q_i^{\lambda_i} - q_i^{\lambda_i - 1}) \prod_{i=1}^{t}(s_i^{\mu_i} - s_i^{\mu_i - 1}) \\
&= \prod_{i=1}^{r} \left[p_i^{\gamma_i + \delta_i} \left(1 - \frac{1}{p_i}\right)^2 \right] \prod_{i=1}^{s}(q_i^{\lambda_i} - q_i^{\lambda_i - 1}) \prod_{i=1}^{t}(s_i^{\mu_i} - s_i^{\mu_i - 1}) \\
&= \prod_{i=1}^{r}(p_i^{\gamma_i} - p_i^{\gamma_i - 1}) \prod_{i=1}^{r}(p_i^{\delta_i} - p_i^{\delta_i - 1}) \prod_{i=1}^{s}(q_i^{\lambda_i} - q_i^{\lambda_i - 1}) \prod_{i=1}^{t}(s_i^{\mu_i} - s_i^{\mu_i - 1}) \\
&= \phi(n \wedge m)\phi(n \vee m)
\end{aligned}$$

□

Ex. 2.19 *Prove that* $\phi(nm)\phi((n,m)) = (n,m)\phi(n)\phi(m)$.

Proof. With the notations of Ex. 2.18,

$$\begin{aligned}
\phi(nm) &= \prod_{i=1}^{r} p_i^{\alpha_i + \beta_i} \left(1 - \frac{1}{p_i}\right) \prod_{i=1}^{s} q_i^{\lambda_i} \left(1 - \frac{1}{q_i}\right) \prod_{i=1}^{t} s_i^{\mu_i} \left(1 - \frac{1}{s_i}\right) \\
\phi(n \wedge m) &= \prod_{i=1}^{r} p_i^{\gamma_i} \left(1 - \frac{1}{p_i}\right)
\end{aligned}$$

so

$$\begin{aligned}
(n \wedge m)\phi(n)\phi(m) &= \prod_{i=1}^{r} p_i^{\gamma_i} \prod_{i=1}^{r} \left[p_i^{\alpha_i + \beta_i} \left(1 - \frac{1}{p_i}\right)^2 \right] \prod_{i=1}^{s} q_i^{\lambda_i} \left(1 - \frac{1}{q_i}\right) \prod_{i=1}^{t} s_i^{\mu_i} \left(1 - \frac{1}{s_i}\right) \\
&= \prod_{i=1}^{r} \left[p_i^{\alpha_i + \beta_i + \gamma_i} \left(1 - \frac{1}{p_i}\right)^2 \right] \prod_{i=1}^{s} q_i^{\lambda_i} \left(1 - \frac{1}{q_i}\right) \prod_{i=1}^{t} s_i^{\mu_i} \left(1 - \frac{1}{s_i}\right) \\
&= \phi(nm)\phi(n \wedge m)
\end{aligned}$$

Conclusion :

$$(n \wedge m)\phi(n)\phi(m) = \phi(nm)\phi(n \wedge m).$$

□

Ex. 2.20 *Prove that* $\prod_{d \mid n} d = n^{\nu(n)/2}$.

Proof. Let

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

the decomposition of n in prime factors.

$$\begin{aligned}
\left(\prod_{d|n} d\right)^2 &= \prod_{d|n} d \prod_{d|n} d \\
&= \prod_{d|n} d \prod_{\delta|n} \frac{n}{\delta} \qquad (\delta = n/d) \\
&= n^{\nu(n)} \prod_{d|n} d \prod_{d|n} \frac{1}{d} \\
&= n^{\nu(n)}
\end{aligned}$$

Conclusion :

$$\prod_{d|n} d = n^{\frac{\nu(n)}{2}}.$$

□

Ex. 2.21 *Define $\wedge(n) = \log p$ if n is a power of p and zero otherwise. Prove that $\sum_{d|n} \mu(n/d) \log d = \wedge(n)$. [Hint: First calculate $\sum_{d|n} \wedge(d)$ and then apply the Möbius inversion formula.]*

Proof.

$$\begin{cases} \wedge(n) = \log p & \text{if } n = p^\alpha,\ \alpha \in \mathbb{N}^* \\ = 0 & \text{otherwise.} \end{cases}$$

Let $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ the decomposition of n in prime factors. As $\wedge(d) = 0$ for all divisors of n, except for $d = p_j^i, i > 0, j = 1, \ldots t$,

$$\begin{aligned}
\sum_{d|n} \wedge(d) &= \sum_{i=1}^{\alpha_1} \wedge(p_1^i) + \cdots + \sum_{i=1}^{\alpha_t} \wedge(p_t^i) \\
&= \alpha_1 \log p_1 + \cdots + \alpha_t \log p_t \\
&= \log n
\end{aligned}$$

By Möbius Inversion Theorem,

$$\wedge(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log d.$$

□

Ex. 2.22 *Show that the sum of all the integers t such that $1 \le t \le n$ and $(t, n) = 1$ is $\frac{1}{2} n \phi(n)$.*

Proof. Suppose $n > 1$ (the formula is false if $n = 1$).

Let $S = \sum\limits_{1 \le t \le n,\ t \wedge n = 1} t = \sum\limits_{1 \le t \le n-1,\ t \wedge n = 1} t.$

Using the symmetry $t \mapsto n-t$, as $t \wedge n = 1 \iff (n-t)\wedge n = 1$, we obtain

$$\begin{aligned}
2S &= \sum_{1\le t\le n-1,\ t\wedge n=1} t + \sum_{1\le t\le n-1,\ t\wedge n=1} t \\
&= \sum_{1\le t\le n-1,\ t\wedge n=1} t + \sum_{1\le s\le n-1,\ (n-s)\wedge n=1} n-s \qquad (s=n-t)\\
&= \sum_{1\le t\le n-1,\ t\wedge n=1} t + \sum_{1\le t\le n-1,\ (n-t)\wedge n=1} n-t \\
&= \sum_{1\le t\le n-1,\ t\wedge n=1} t + \sum_{1\le t\le n-1,\ t\wedge n=1} n-t \\
&= \sum_{1\le t\le n-1,\ t\wedge n=1} n \\
&= n \ \mathrm{Card}\{t\in\mathbb{N} \mid 1\le t\le n-1, t\wedge n=1\}\\
&= n\phi(n)
\end{aligned}$$

Conclusion :

$$\forall n\in\mathbb{N}^*, \quad \sum_{1\le t\le n,\ t\wedge n=1} t = \frac{1}{2}n\phi(n).$$

(See another interesting proof in Adam Michalik's paper.)

□

Ex. 2.23 *Let $f(x)\in\mathbb{Z}[x]$ and let $\psi(n)$ be the number of $f(j), j=1,2,\ldots,n$, such that $(f(j),n)=1$. Show that $\psi(n)$ is multiplicative and that $\psi(p^t)=p^{t-1}\psi(p)$. Conclude that $\psi(n)=n\prod_{p\mid n}\psi(p)/p$.*

Proof. My interpretation of this statement is that $\psi(n)$ is the number of $j, j=1,2,\ldots,n$, such that $(f(j),n)=1$ (if f is not one to one, we may obtain a different value).

Let $A_n=\{j\in\mathbb{Z}, 1\le j\le n \mid f(j)\wedge n=1\}$: then $\psi(n)=|A_n|$. If $f(x)=\sum_{k=0}^d a_k x^k$, note $f_n(x)\in(\mathbb{Z}/n\mathbb{Z})[x]$ the polynomial $f_n(x)=\sum_{k=0}^n [a_k]_n x^k$ (here, we represent the class of $j\in\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ by $[j]_n$). We can write without inconvenient $f=f_n$.

Let $B_n=\{a\in\mathbb{Z}/n\mathbb{Z} \mid f(a)\in(\mathbb{Z}/n\mathbb{Z})^*\}$, where $(\mathbb{Z}/n\mathbb{Z})^*$ is the group of invertible elements of $\mathbb{Z}/n\mathbb{Z}$.

Then $u: A_n\to B_n, j\mapsto [j]_n$ is a bijection.

Indeed u is well defined : if $j\in A_n, f(j)\wedge n=1$, so $f([j]_n)=[f(j)]_n\in(\mathbb{Z}/n\mathbb{Z})^*$.

u is injective : $[j]_n=[k]_n$ with $1\le j\le n, 1\le k\le n$ implies $j=k$.

u is surjective : if $a\in\mathbb{Z}/n/Z$ verifies $f(a)\in(\mathbb{Z}/n\mathbb{Z})^*$, let j the unique representative of a such that $1\le j\le n$. Then $f(j)\wedge n=1$, so $u(j)=a$.

Thus

$$\psi(n)=|B_n|, \text{ where } B_n=\{a\in\mathbb{Z}/n\mathbb{Z} \mid f(a)\in(\mathbb{Z}/n\mathbb{Z})^*\}.$$

Suppose $n\wedge m=1$. Let

$$\varphi:\left\{\begin{array}{ccc} B_{nm} & \to & B_n\times B_m\\ {[j]_{nm}} & \mapsto & ([j]_n,[j]_m)\end{array}\right.$$

• φ is well defined : $[j]_{nm}=[k]_{nm}\Rightarrow j\equiv k \pmod{nm} \Rightarrow (j\equiv k \pmod n, j\equiv k \pmod m)\Rightarrow ([j]_n,[j]_m)=([k]_n,[k]_m)$.

• φ is injective : if $\varphi([j]_{nm})=\varphi([k]_{nm})$, then $[j]_n=[k]_n, [j]_m=[k]_m$, so $n\mid j-k, m\mid j-k$. As $n\wedge m=1, nm\mid j-k$ so $[j]_{nm}=[k]_{nm}$.

• φ is surjective : if $(a,b) \in B_n \times B_m$, there exist $j,k \in \mathbb{Z}, 1 \le j \le n, 1 \le j \le m$, such that $a = [j]_n, b = [k]_n$. From the Chinese Remainder Theorem, there exists $i \in \mathbb{Z}, 1 \le i \le n$, such that $i \equiv j \pmod n, i \equiv k \pmod m$. Then $\varphi([i]_{nm}) = ([i]_n, [i]_m) = ([j]_n, [k]_m) = (a,b)$.

Finally, $\psi(nm) = |B_{nm}| = |B_n|\,|B_m| = \psi(n)\psi(m)$, if $n \wedge m = 1$: ψ is a multiplicative function.

The interval $I = [1, p^t]$ is the disjoint reunion of the p^{t-1} intervals $I_k = [kp+1, (k+1)p]$ for $k = 0, 1, \cdots, p^{t-1} - 1$, so $\psi(p^t) = \sum\limits_{k=0}^{p^{t-1}-1} \operatorname{Card} C_k$, where $C_k = \{j \in I_k |\ f(j) \wedge p^t = 1\} = \{j \in I_k |\ f(j) \wedge p = 1\}$.

As $f(j) \wedge p = 1 \iff f(j-kp) \wedge p = 1$, the application $v : C_k \to C_0, j \mapsto j - kp$ is well defined and is bijective, so $|C_k| = |C_0| = \psi(p)$. Thus $\psi(p^t) = p^{t-1} \operatorname{Card} I_0 = p^{t-1}\psi(p)$:

$$\psi(p^t) = p^{t-1}\psi(p).$$

If $n = \prod_{p|n} p^{t(p)}$, then

$$\begin{aligned}
\psi(n) &= \prod_{p|n} \psi(p^{t(p)}) \\
&= \prod_{p|n} p^{t(p)-1}\psi(p) \\
&= n \prod_{p|n} \frac{\psi(p)}{p}
\end{aligned}$$

□

Ex. 2.24 *Supply the details to the proof of Theorem 3.*

As Adam Michalik, I suppose that there is a misprint, we must prove Theorem 4 :
Let k a finite field with q elements.
$\sum q^{-\deg p(x)}$ diverges, where the sum is over all monic irreducible $p(x)$ in $k[x]$.

Proof. Notations :

$\mathcal{P}$: set of all monic polynomials p in $k[x]$.

$\mathcal{P}_n$: set of all monic polynomials p in $k[x]$ with $\deg(p) \le n$.

$\mathcal{M}$: set of all monic irreducible polynomials p in $k[x]$.

We must prove that $\sum\limits_{p \in \mathcal{M}} q^{-\deg p(x)}$ diverges.

• $\sum\limits_{f \in \mathcal{P}} q^{-\deg f}$ diverges :

$$\begin{aligned}
\sum_{f \in \mathcal{P}_n} \frac{1}{q^{\deg f}} &= \sum_{d=0}^{n} \sum_{\deg(f)=d} \frac{1}{q^d} \\
&= \sum_{d=0}^{n} \frac{1}{q^d} \operatorname{Card}\{f \in \mathcal{P} \mid \deg(f) = d\} \\
&= \sum_{d=0}^{n} \frac{1}{q^d}\, q^d = n + 1.
\end{aligned}$$

So $\sum\limits_{f \in \mathcal{P}} q^{-\deg f}$ diverges.

• $\sum\limits_{f\in\mathcal{P}} q^{-2\deg f}$ converges :

$$\begin{aligned}\sum_{f\in\mathcal{P}_n} q^{-2\deg(f)} &= \sum_{d=0}^{n} \sum_{\deg(f)=d} \frac{1}{q^{2d}} \\ &= \sum_{d=0}^{n} \frac{1}{q^{2d}} \operatorname{Card}\{f\in\mathcal{P} \mid \deg(f)=d\} \\ &= \sum_{d=0}^{n} \frac{1}{q^{d}} \\ &\le \frac{1}{1-\frac{1}{q}}\end{aligned}$$

As any finite subset of $\mathcal{P}$ is included in some $\mathcal{P}_n$, $\sum\limits_{f\in\mathcal{P}} q^{-2\deg f}$ converges.

• $\sum q^{-\deg p(x)}$ diverges :

Let $\mathcal{P}_n = \{p_1, p_2, \ldots, p_{l(n)}\}$ the set of all monic irreducible polynomials such that $\deg p_i \le n$. Let

$$\lambda(n) = \prod_{i=1}^{l(n)} \frac{1}{1-\frac{1}{q^{\deg(p_i)}}}.$$

For simplicity, we write $l = l(n)$ for a fixed $n\in\mathbb{N}$. Then

$$\begin{aligned}\lambda(n) &= \prod_{i=1}^{l} \sum_{a_i=0}^{\infty} \frac{1}{q^{a_i \deg p_i}} \\ &= \left(1+\frac{1}{q^{\deg p_1}}+\frac{1}{q^{\deg p_1^2}}+\cdots\right)\times\cdots\times\left(1+\frac{1}{q^{\deg p_l}}+\frac{1}{q^{\deg p_l^2}}+\cdots\right) \\ &= \sum_{(a_1,\cdots,a_j)\in\mathbb{N}^l} \frac{1}{q^{\deg(p_1^{a_1}\cdots p_l^{a_l})}}\end{aligned}$$

Since the monic prime factors of any polynomial $p\in\mathcal{P}_n$ are in $\mathcal{P}_n$, the decomposition of p is $p = p_1^{a_1}\cdots p_l^{a_l}$, so

$$\lambda(n) \ge \sum_{p\in\mathcal{P}_n} \frac{1}{q^{\deg p}} = n+1.$$

So $\lim\limits_{n\to\infty} \lambda(n) = \infty$: this is another proof that there exist infinitely many monic irreducible polynomials in $k[x]$ (cf Ex. 2.1).

$$\begin{aligned}\log\lambda(n) &= -\sum_{i=1}^{l(n)} \log\left(1-\frac{1}{q^{\deg p_i}}\right) \\ &= \sum_{i=1}^{l(n)} \sum_{m=1}^{\infty} \frac{1}{mq^{m\deg p_i}} \\ &= \frac{1}{q^{\deg p_1}}+\cdots+\frac{1}{q^{\deg p_{l(n)}}}+\sum_{i=1}^{l(n)} \sum_{m=2}^{\infty} \frac{1}{mq^{m\deg p_i}}\end{aligned}$$

Yet

$$\sum_{m=2}^{\infty} \frac{1}{mq^{m \deg p_i}} \leq \sum_{m=2}^{\infty} \frac{1}{q^{m \deg p_i}}$$
$$= \frac{1}{q^{2 \deg p_i}} \frac{1}{1 - \frac{1}{q^{deg p_i}}}$$
$$= \frac{1}{q^{2 \deg p_i} - q^{\deg p_i}} \leq \frac{2}{q^{2 \deg p_i}}$$

(the last inequality is equivalent to $2 \leq q^{\deg p_i}$). So

$$\log \lambda(n) \leq \frac{1}{q^{\deg p_1}} + \cdots + \frac{1}{q^{\deg p_{l(n)}}} + 2 \left(\frac{1}{q^{2 \deg p_1}} + \cdots + \frac{1}{q^{2 \deg p_{l(n)}}} \right).$$

As $\frac{1}{q^{2 \deg p_1}} + \cdots + \frac{1}{q^{2 \deg p_{l(n)}}}$ is less than the constant $\sum_{f \in \mathcal{P}} q^{-2 \deg f}$, if $\sum_{p \in \mathcal{M}} q^{-\deg p(x)}$ converges, then $\log \lambda(n) \leq C$, where C is a constant, so $\lambda(n) \leq e^C$ for all $n \in \mathbb{N}$, in contradiction with $\lim_{n \to \infty} \lambda(n) = \infty$.

Conclusion : $\sum_{p \in \mathcal{M}} q^{-\deg p(x)}$ diverges. □

Ex. 2.25 *Consider the function $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$. ζ is called the Riemann zeta function. It converges for $s > 1$. Prove the formal identity (Euler's identity)*

$$\zeta(s) = \prod_p (1 - 1/p^s)^{-1}.$$

Proof. We prove this equality, not only formally, but for all complex value s such that $\mathrm{Re}(s) > 1$.

Let $s \in \mathbb{C}$ and $f(n) = \frac{1}{n^s}$, $n \in \mathbb{N}^*$.

f is completely multiplicative : $f(mn) = f(m)f(n)$ for $m, n \in \mathbb{N}^*$.

Moreover $\sum_{n=1}^{\infty} f(n)$ is absolutely convergent for $\mathrm{Re}(s) > 1$. Indeed, If $s = u + iv, u, v \in \mathbb{R}$, $|f(n)| = |n^{-s}| = |e^{-s \log(n)}| = |e^{-u \log(n)} e^{-iv \log(n)}| = e^{-u \log(n)} = \frac{1}{n^u}$, so $\sum_{n=1}^{\infty} |f(n)| = 1/n^u$ converges if $u = \mathrm{Re}(s) > 1$.

With these properties of f (f multiplicative and $\sum_{n=1}^{\infty} f(n)$ absolutely convergent), we will show that

$$\sum_{n=1}^{\infty} f(n) = \prod_p (1 + f(p) + f(p^2) + \cdots).$$

Let $S^* = \sum_{n=1}^{\infty} |f(n)| < \infty$, and $S = \sum_{n=1}^{\infty} f(n) \in \mathbb{C}$. For each prime number p, $\sum_{k=1}^{\infty} |f(p^k)|$ converges (this sum is less than S^*), so $\sum_{k=0}^{\infty} f(p^k)$ converges absolutely. Thus, for $x \in \mathbb{R}$, the two finite products

$$P(x) = \prod_{p \leq x} \sum_{k=0}^{\infty} f(p^k), \qquad P^*(x) = \prod_{p \leq x} \sum_{k=0}^{\infty} |f(p^k)|$$

are well defined.

If p, q are two prime numbers, as $\sum_{i=0}^{\infty} f(p^i), \sum_{j=0}^{\infty} f(q^j)$ are absolutely convergent, $(f(p^i)f(q^j))_{(i,j)\in\mathbb{N}^2}$ is sommable, so the sum of these elements can be arranged in any order :

$$\sum_{i=0}^{\infty} f(p^i) \sum_{k=0}^{\infty} f(q^k) = \sum_{(i,j)\in\mathbb{N}^2} f(p^i)f(q^j) = \sum_{(i,j)\in\mathbb{N}^2} f(p^i q^j).$$

If $p_1, \cdots, p_t$ are all the prime $p \leq x$, repeating t times these products, we obtain

$$\begin{aligned}
P(x) &= \prod_{p\leq x} \sum_{k=0}^{\infty} f(p^k) \\
&= \sum_{i_1=0}^{\infty} f(p_1^{i_1}) \cdots \sum_{i_t=0}^{\infty} f(p_t^{i_t}) \\
&= \sum_{(i_1,\ldots,i_k)\in\mathbb{N}^k} f(p_1^{i_1} \cdots p_t^{i_t}) \\
&= \sum_{n\in\Delta} f(n),
\end{aligned}$$

where Δ is the set of integers $n \in \mathbb{N}^*$ whose prime factors are not greater than x. Let $\overline{\Delta} = \mathbb{N}^* \setminus \Delta :$ this is the set of numbers $n \in \mathbb{N}^*$ such that at least a prime factor is greater than x. So

$$P(x) = \sum_{n\in\Delta} f(n) = S - \sum_{n\in\overline{\Delta}} f(n).$$

Then

$$|P(x) - S| \leq \sum_{n\in\overline{\Delta}} |f(n)| \leq \sum_{n\geq x} |f(n)|.$$

So $\lim\limits_{x\to+\infty} P(x) = S$, that is

$$\prod_p \sum_{k=0}^{\infty} f(p^k) = \sum_{n=1}^{\infty} f(n).$$

Finally,

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{1}{n^s} &= \prod_p \left(1 + \frac{1}{p^s} + \cdots + \frac{1}{p^{ks}} + \cdots\right) \\
&= \prod_p (1 - 1/p^s)^{-1}
\end{aligned}$$

□

Ex. 2.26 *Verify the formal identities:*

(a) $\zeta(s)^{-1} = \sum \mu(n)/n^s$

(b) $\zeta(s)^2 = \sum \nu(n)/n^s$

(c) $\zeta(s)\zeta(s-1) = \sum \sigma(n)/n^s$

Proof. Without any consideration of convergence :

(a)

$$\begin{aligned}
\zeta(s)\sum_{m=1}^{\infty}\frac{\mu(m)}{m^s} &= \sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{m=1}^{\infty}\frac{\mu(m)}{m^s}\\
&= \sum_{n,m\geq 1}\frac{\mu(m)}{n^s m^s}\\
&= \sum_{u=1}^{\infty}\sum_{m\mid u}\mu(m)\frac{1}{u^s} \qquad\qquad (u=nm)\\
&= \sum_{u=1}^{\infty}\frac{1}{u^s}\sum_{m\mid u}\mu(m)\\
&= 1
\end{aligned}$$

Indeed, $\sum_{m\mid u}\mu(m) = 1$ if $u=1$, 0 otherwise. So

$$\zeta(s)^{-1} = \sum_{n\in\mathbb{N}^*}\mu(n)/n^s.$$

(b)

$$\begin{aligned}
\zeta(s)^2 &= \sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{m=1}^{\infty}\frac{1}{m^s}\\
&= \sum_{n,m\geq 1}\frac{1}{(nm)^s}\\
&= \sum_{u\geq 1}\sum_{n\mid u}\frac{1}{u^s}\\
&= \sum_{u\geq 1}\frac{1}{u^s}\sum_{n\mid u}1\\
&= \sum_{u\geq 1}\frac{1}{u^s}\nu(u)
\end{aligned}$$

So

$$\zeta(s)^2 = \sum_{n=1}^{\infty}\frac{\nu(n)}{n^s}.$$

(c) For $\mathrm{Re}(s) > 2$,

$$\begin{aligned}
\zeta(s)\zeta(s-1) &= \sum_{n\geq 1}\frac{1}{n^s}\sum_{m\geq 1}\frac{1}{m^{s-1}}\\
&= \sum_{m,n\geq 1}\frac{m}{(nm)^s}\\
&= \sum_{u\geq 1}\left(\sum_{m\mid u} m\right)\frac{1}{u^s}\\
&= \sum_{u\geq 1}\frac{\sigma(u)}{u^s}
\end{aligned}$$

So

$$\zeta(s)\zeta(s-1) = \sum_{n\geq 1} \frac{\sigma(n)}{n^s}.$$

□

Ex. 2.27 *Show that $\sum 1/n$, the sum being over square free integers, diverges. Conclude that $\prod_{p<N}(1+1/p) \to \infty$ as $N \to \infty$. Since $e^x > 1 + x$, conclude that $\sum_{p<N} 1/p \to \infty$. (This proof is due to I.Niven.)*

Proof. Let $S \subset \mathbb{N}^*$ the set of square free integers.

Let $N \in \mathbb{N}^*$. Every integer n, $1 \leq n \leq N$ can be written as $n = ab^2$, where a, b are integers and a is square free. Then $1 \leq a \leq N$, and $1 \leq b \leq \sqrt{N}$, so

$$\sum_{n\leq N} \frac{1}{n} \leq \sum_{a\in S, a\leq N} \sum_{1\leq b\leq\sqrt{N}} \frac{1}{ab^2} \leq \sum_{a\in S, a\leq N} \frac{1}{a} \sum_{b=1}^{\infty} \frac{1}{b^2} = \frac{\pi^2}{6} \sum_{a\in S, a\leq N} \frac{1}{a}.$$

So

$$\sum_{a\in S, a\leq N} \frac{1}{a} \geq \frac{6}{\pi^2} \sum_{n\leq N} \frac{1}{n}.$$

As $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges, $\lim\limits_{N\to\infty} \sum\limits_{a\in S, a\leq N} \frac{1}{a} = +\infty$, so the family $\left(\frac{1}{a}\right)_{a\in S}$ of the inverse of square free integers is not summable.

Let $S_N = \prod_{p<N}(1+1/p)$, and $p_1, p_2, \ldots, p_l$ $(l = l(N))$ all prime integers less than N. Then

$$\begin{aligned} S_N &= \left(1 + \frac{1}{p_1}\right) \cdots \left(1 + \frac{1}{p_l}\right) \\ &= \sum_{(\varepsilon_1, \cdots, \varepsilon_l)\in\{0,1\}^l} \frac{1}{p_1^{\varepsilon_1} \cdots p_l^{\varepsilon_l}} \end{aligned}$$

We prove this last formula by induction. This is true for $l = 1 : \sum_{\varepsilon\in\{0,1\}} 1/p_1^{\varepsilon} = 1 + 1/p_1$.

If it is true for the integer l, then

$$\begin{aligned} \left(1 + \frac{1}{p_1}\right) \cdots \left(1 + \frac{1}{p_l}\right)\left(1 + \frac{1}{p_{l+1}}\right) &= \sum_{(\varepsilon_1,\ldots,\varepsilon_l)\in\{0,1\}^l} \frac{1}{p_1^{\varepsilon_1} \cdots p_l^{\varepsilon_l}} \left(1 + \frac{1}{p_{l+1}}\right) \\ &= \sum_{(\varepsilon_1,\ldots,\varepsilon_l)\in\{0,1\}^l} \frac{1}{p_1^{\varepsilon_1} \cdots p_l^{\varepsilon_l}} + \sum_{(\varepsilon_1,\ldots,\varepsilon_l)\in\{0,1\}^l} \frac{1}{p_1^{\varepsilon_1} \cdots p_l^{\varepsilon_l} p_{l+1}} \\ &= \sum_{(\varepsilon_1,\ldots,\varepsilon_l,\varepsilon_{l+1})\in\{0,1\}^{l+1}} \frac{1}{p_1^{\varepsilon_1} \cdots p_l^{\varepsilon_l} p_{l+1}^{\varepsilon_{l+1}}} \end{aligned}$$

So it is true for all l.

Thus $S_N = \sum_{n\in\Delta} \frac{1}{n}$, where Δ is the set of square free integers whose prime factors are less than N.

As $\sum 1/n$, the sum being over square free integers, diverges, $\lim\limits_{N\to\infty} S_N = +\infty$:

$$\lim_{N\to\infty} \prod_{p<N} \left(1 + \frac{1}{p}\right) = +\infty.$$

$e^x \geq 1 + x, x \geq \log(1 + x)$ for $x > 0$, so

$$\log S_N = \sum_{k=1}^{l(N)} \log\left(1 + \frac{1}{p_k}\right) \leq \sum_{k=1}^{l(N)} \frac{1}{p_k}.$$

$\lim_{N\to\infty} \log S_N = +\infty$ and $\lim_{N\to\infty} l(N) = +\infty$, so

$$\lim_{N\to\infty} \sum_{p<N} \frac{1}{p} = +\infty.$$

$\square$

3 Chapter 3

Ex. 3.1 *Show that there are infinitely many primes congruent to -1 modulo 6.*

Proof. Let n any integer such that $n \geq 3$, and $N = n! - 1 = 2 \times 3 \times \cdots \times n - 1 > 1$.

Then $N \equiv -1 \pmod 6$. As $N + 2, N + 3, N + 4$ are composite, every prime factor of N is congruent to 1 or -1 modulo 6. If every prime factor of N was congruent to 1, then $N \equiv 1 \pmod 6$: this is a contradiction because $-1 \not\equiv 1 \pmod 6$. So there exists a prime factor p of N such that $p \equiv -1 \pmod 6$.

If $p \leq n$, then $p \mid n!$, and $p \mid N = n! - 1$, so $p \mid 1$. As p is prime, this is a contradiction, so $p > n$.

Conclusion :

for any integer n, there exists a prime $p > n$ such that $p \equiv -1 \pmod 6$: there are infinitely many primes congruent to -1 modulo 6. $\square$

Ex. 3.2 *Construct addition and multiplication tables for $\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}$, and $\mathbb{Z}/10\mathbb{Z}$.*

Proof. More a latex exercise than a mathematical one.

$\mathbb{Z}/5\mathbb{Z}$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}/8\mathbb{Z}$:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

$\mathbb{Z}/10\mathbb{Z}$:

$+$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

$\times$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Python code to generate the latex code to create such an array :

```
n= 10

print('$')
ligne = '\\begin{array}{c|'+ n*'c'+'}'
print(ligne)
ligne='\\times'
for j in range(n):
    ligne += ' & ' + str(j)
ligne += '\\'
ligne += '\\'
ligne += ' \\hline'
print(ligne)
for i in range(n):
    ligne = str(i)
    for j in range(n):
        ligne +=' & '+ str((i * j) % n)
    ligne += '\\'
    ligne += '\\'
    print(ligne)
print('\\end{array}')
print('$')
```

□

Ex. 3.3 *Let abc be the decimal representation for an integer between* 1 *and* 1000*. Show that abc is divisible by* 3 *iff* $a+b+c$ *is divisible by* 3*. Show that the same result is true if we replace* 3 *by* 9*. Show that abc is divisible by* 11 *iff* $a-b+c$ *is divisible by* 11*. Generalize to any number written in decimal notation.*

Proof. Let $n = \overline{abc}$ the decimal representation of n.

As $10 \equiv 1 \pmod 3$, $10^3 \equiv 10^2 \equiv 10 \equiv 1 \pmod 3$, so

$$\begin{aligned} 3 \mid n &\iff 10^3 a + 10^2 b + c \equiv 0 \pmod 3 \\ &\iff a + b + c \equiv 0 \pmod 3 \qquad\qquad 3 \mid a+b+c \end{aligned}$$

As $10 \equiv 1 \pmod 9$ the same demonstration is true for the result

$$9 \mid n \iff 9 \mid a + b + c.$$

Similarly, $10 \equiv -1 \pmod{11}$, and $10^2 \equiv 1, 10^3 \equiv -1$, so

$$\begin{aligned} 11 \mid n &\iff 10^3 a + 10^2 b + c \equiv 0 \pmod 11 \\ &\iff a - b + c \equiv 0 \pmod 3 \end{aligned}$$

More generally, let $n = \overline{a_l a_{l-1} \cdots a_0}$ is the decimal representation of n.

$10^n \equiv 1 \pmod 9$, so

$$\begin{aligned} 9 \mid n &\iff \sum_{k=0}^{l} a_k 10^k \equiv 0 \pmod 9 \\ &\iff \sum_{k=0}^{l} a_k \equiv 0 \pmod 9 \\ &\iff 9 \mid a_0 + a_1 + \cdots + a_n \end{aligned}$$

□

Ex. 3.4 *Show that the equation $3x^2 + 2 = y^2$ has no solution in integers.*

Proof. If $3x^2 + 2 = y^2$, then $\overline{y}^2 = \overline{2}$ in $\mathbb{Z}/3\mathbb{Z}$.

As $\{-1, 0, 1\}$ is a complete set of residues modulo 3, the squares in $\mathbb{Z}/3\mathbb{Z}$ are $\overline{0} = \overline{0}^2$ and $\overline{1} = \overline{1}^2 = (\overline{-1})^2$, so $\overline{2}$ is not a square in $\mathbb{Z}/3\mathbb{Z}$: $\overline{y}^2 = \overline{2}$ is impossible in $\mathbb{Z}/3\mathbb{Z}$.

Thus $3x^2 + 2 = y^2$ has no solution in integers. □

Ex. 3.5 *Show that the equation $7x^2 + 2 = y^3$ has no solution in integers.*

Proof. If $7x^2 + 2 = y^3,\ x, y \in \mathbb{Z}$, then $y^3 \equiv 2 \pmod 7$ (so $y \not\equiv 0 \pmod 7$)

From Fermat's Little Theorem, $y^6 \equiv 1 \pmod 7$, so $2^2 \equiv y^6 \equiv 1 \pmod 7$, which implies $7 \mid 2^2 - 1 = 3$: this is a contradiction. Thus the equation $7x^2 + 2 = y^3$ has no solution in integers. □

Ex. 3.6 *Let an integer $n > 0$ be given. A set of integers $a_1, \ldots, a_{\phi(n)}$ is called a reduced residue system modulo n if they are pairwise incongruent modulo n and $(a_i, n) = 1$ for all i. If $(a, n) = 1$, prove that $aa_1, aa_2, \ldots, aa_{\phi(n)}$ is again a reduced residue system modulo n.*

Proof. Let $a_1, \ldots, a_{\phi(n)}$ a reduced residue system modulo n.

- As $a \wedge n = 1$ and $a_i \wedge n = 1,\ i = 1, 2, \ldots, \phi(n)$, then $aa_i \wedge n = 1$.
- As $a \wedge n = 1$, there exists $a' \in \mathbb{Z}$ such that $aa' \equiv 1 \pmod n$. then

$$aa_i \equiv aa_j \Rightarrow a'aa_i \equiv a'au_j \pmod n \Rightarrow a_i \equiv a_j \pmod n.$$

So $i \neq j \Rightarrow a_i \not\equiv a_j \Rightarrow aa_i \not\equiv aa_j$:

$aa_1, \ldots, aa_{\phi(n)}$ a reduced residue system modulo n.

Note that $\{a_1, a_2, \ldots, a_{\phi(n)}\}$ is a reduced residue system modulo n if and only if $\{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_{\phi(n)}}\} = U(\mathbb{Z}/n\mathbb{Z})$. □

Ex. 3.7 *Use Ex. 2.6 to give another proof of Euler's theorem, $a^{\phi(n)} \equiv 1 \pmod n$ for $(a, n) = 1$.*

Proof. The proof is more clear if we stay in $\mathbb{Z}/n\mathbb{Z}$.

Let $P = \prod_{x \in U(\mathbb{Z}/n\mathbb{Z})} x$

(if $\{a_1, \ldots, a_{\phi(n)}\}$ is a reduced residue system modulo n, then $\overline{P} = \prod_{i=1}^{\phi(n)} a_i$.)

Let $a \in \mathbb{Z}$ such that $a \wedge n = 1$, then $b = \overline{a} \in U(\mathbb{Z}/n\mathbb{Z})$, and

$$\psi \left\{ \begin{array}{ccc} U(\mathbb{Z}/n\mathbb{Z}) & \to & U(\mathbb{Z}/n\mathbb{Z}) \\ x & \mapsto & bx \end{array} \right.$$

• $\psi(x) = \psi(x') \Rightarrow bx = bx' \Rightarrow b^{-1}bx = b^{-1}ax' \Rightarrow x = x'$ so ψ is injective.
• Let $y \in U(\mathbb{Z}/n\mathbb{Z})$. If $x = b^{-1}y$, then $\psi(x) = bb^{-1}y = y$, so ψ is surjective.
ψ is a bijection, so

$$\prod_{x \in U(\mathbb{Z}/n\mathbb{Z})} bx = \prod_{x \in U(\mathbb{Z}/n\mathbb{Z})} x,$$

that is

$$b^{\phi(n)} \prod_{x \in U(\mathbb{Z}/n\mathbb{Z})} x = \prod_{x \in U(\mathbb{Z}/n\mathbb{Z})} x.$$

As $\prod_{x \in U(\mathbb{Z}/n\mathbb{Z})} x$ is invertible,

$$b^{\phi(n)} = 1.$$

That is $\overline{a}^{\phi(n)} = 1$: for all $a \in \mathbb{Z}$, if $a \wedge n = 1$, then $a^{\phi(n)} \equiv 1 \pmod n$. □

Ex. 3.8 *Let p be an odd prime. If $k \in \{1, 2, \ldots, p-1\}$, show that there is a unique b_k in this set such that $kb_k \equiv 1 \pmod p$. Show that $k \neq b_k$ unless $k = 1$ or $k = p - 1$.*

Proof. • existence.

As p is prime and $1 \leq k \leq p-1$, $k \wedge p = 1$, so there exist $\lambda_k, \mu_k \in \mathbb{Z}$ such that $\lambda_k p + \mu_k k = 1$. Let $b_k \in \{0, 1, \ldots, p-1\}$ such that $b_k \equiv \mu_k \pmod p$. Then $kb_k \equiv 1$, and $b_k \not\equiv 0 \pmod p$, so $1 \leq b_k \leq p - 1$.

• unicity. If $kb_k \equiv kb'_k \pmod p$, where $b_k, b'_k \in \{1, 2, \ldots, p-1\}$, then $p \mid k(b'_k - b_k)$, and $p \wedge k = 1$, so $p \mid b'_k - b_k$. $b'_k \equiv b_k$, and $b_k, b'_k \in \{1, 2, \ldots, p-1\}$, so $b_k = b'_k$.

If p is a prime number, and $k \in \{1, 2, \ldots, p-1\}$, there is a unique b_k in $\{1, 2, \ldots, p-1\}$ such that $kb_k \equiv 1 \pmod p$.

If $k = b_k$, then $k^2 \equiv 1 \pmod p$, so $p \mid (k-1)(k+1)$, and p is a prime, thus $p \mid k - 1$ or $p \mid k + 1$, that is $k \equiv \pm 1 \pmod p$. As $1 \leq k \leq p - 1$, $k = 1$ or $k = p - 1$ (and $1^2 \equiv (p-1)^2 \equiv 1 \pmod p$). □

Ex. 3.9 *Use Ex. 3.8 to prove that $(p-1)! \equiv -1 \pmod p$. (misprint corrected)*

Proof. Each element k in the product $p!$ can be associated with its inverse b_k modulo k, except 1 and $p - 1$, which are their own inverse, so

$$p! \equiv 1 \times (p-1) \equiv -1 \pmod p.$$

□

Ex. 3.10 *If n is not a prime, show that $(n-1)! \equiv 0 \pmod n$, except when $n = 4$.*

Proof. Suppose that $n > 1$ is not a prime. Then $n = uv$, where $2 \le u \le v \le n-1$.

• If $u \ne v$, then $n = uv \mid (n-1)! = 1 \times 2 \times \cdots \times u \times \cdots \times v \times \cdots \times (n-1)$ (even if $u \wedge v \ne 1$!).

• If $u = v$, $n = u^2$ is a square.

If u is not prime, $u = st$, $2 \le s \le t \le u-1 \le n-1$, and $n = u'v'$, where $u' = s, v' = st^2$ verify $2 \le u' < v' \le n-1$. As in the first case, $n = u'v' \mid (n-1)!$.

If $u = p$ is a prime, then $n = p^2$.

In the case $p = 2$, $n = 4$ and $n = 4 \nmid (n-1)! = 6$. In the other case $p > 2$, and $(n-1)! = (p^2-1)!$ contains the factors $p < 2p < p^2$, so $p^2 \mid (p^2-1)!, n \mid (n-1)!$.

Conclusion : if n is not a prime, $(n-1)! \equiv 0 \pmod n$, except when $n = 4$.

□

Ex. 3.11 *Let $a_1, \ldots, a_{\phi(n)}$ be a reduced residue system modulo n and let N be the number of solutions to $x^2 \equiv 1 \pmod n$. Prove that $a_1 \cdots a_{\phi(n)} \equiv (-1)^{N/2} \pmod n$.*

Proof. If $n = 2$, then $N = 1$ and the result is false. So we suppose $n > 2$.

Let H the subset of $\mathbb{Z}/n\mathbb{Z}$ of all $x \in \mathbb{Z}/n\mathbb{Z}$ such that $x^2 = 1$:

$$H = \{x \in \mathbb{Z}/n\mathbb{Z} \mid x^2 = 1\}$$

(here $1 = \overline{1}$).

$H \subset U(\mathbb{Z}/n\mathbb{Z})$, and $x \in H, y \in H \Rightarrow x^2 = y^2 = 1 \Rightarrow (xy^{-1})^2 = 1 \Rightarrow xy^{-1} \in H$, so H is a subgroup of $(U(\mathbb{Z}/n\mathbb{Z}), \times)$, and $N = \operatorname{Card} H$.

Each $x \in U(\mathbb{Z}/n\mathbb{Z})$ such that $x \notin H$ can be paired with its inverse x^{-1}, and $xx^{-1} = 1$, so

$$P := \prod_{x \in U(\mathbb{Z}/n\mathbb{Z})} x = \prod_{x \in H} x.$$

If $x \in H, -x \in H$.

• If n is odd, each $x = \overline{a} \in H (a \in \mathbb{Z}, 1 \le a \le n-1)$ satisfy $-x \ne x$: otherwise $2a \equiv 0 \pmod n, 2a = kn, k \in \mathbb{Z}$. As $0 < 2a = kn < 2n$, then $k = 1$, and $n = 2a$ is even, which is in contradiction with the hypothesis.

So we each $x \in H$ can be paired with $-x$ in the product P, and $x(-x) = -1$, so

$$P = \prod_{x \in H} x = (-1)^{N/2}.$$

• If n is even, if $x = \overline{a} \in H$ $(a \in \mathbb{Z}, 1 \le a \le n-1)$ satisfy $x = -x$, then $0 < a = k\frac{n}{2} < n$, so $a = \frac{n}{2}$, and $x = \overline{\left(\frac{n}{2}\right)}$ is the only element in Z/nZ such that $x = -x$. $\overline{2}x = \overline{0}$, and $x \in H$, so $\overline{2}x^2 = \overline{0}, \overline{2} = \overline{0}$: since $n > 2$, this is impossible, so $x \ne -x$ for all $x \in H$, and $\prod_{x \in H} x = (-1)^{N/2}$.

Conclusion : if $n > 2$,

$$\prod_{x \in U(\mathbb{Z}/n\mathbb{Z})} x = (-1)^{N/2}.$$

If $a_1, \ldots, a_{\phi(n)}$ is a reduced residue system modulo n, then $\overline{a_1 \cdots a_{\phi(n)}} = P = \prod_{x \in U(\mathbb{Z}/n\mathbb{Z})} x = (-1)^{N/2}$, so

$$a_1 \cdots a_{\phi(n)} \equiv (-1)^{N/2}.$$

□

Ex. 3.12 *Let* $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ *be a binomial coefficient, and suppose* p *is prime. If* $1 \le k \le p-1$*, show that* p *divides* $\binom{p}{k}$*. Deduce* $(a+b)^p \equiv a^p + b^p \pmod p$*.*

Proof. $p \mid p! = k!(p-k)!\binom{p}{k}$.

If $1 \le k \le p-1$, then for each $i, 1 \le i \le k$, $1 \le i < p$, so $i \wedge p = 1$. Thus $\left(\prod_{i=1}^{k} i\right) \wedge p = 1, k! \wedge p = 1$. Similarly, $p-k < p$, so $\left(\prod_{i=1}^{p-k} i\right) \wedge p = 1, (p-k)! \wedge p = 1$. Thus $p \wedge k!(p-k)! = 1$, and $p \mid p! = k!(p-k)!\binom{p}{k}$, so $p \mid \binom{p}{k}$.

Finally, from binomial formula

$$\begin{aligned}(a+b)^p &= a^p + \sum_{k=1}^{p-1}\binom{p}{k} a^k b^{n-k} + b^p \\ &\equiv a^p + b^p \pmod p\end{aligned}$$

□

Ex. 3.13 *Use Ex. 3.12 to give another proof of Fermat's theorem,* $a^{p-1} \equiv 1 \pmod p$ *if* p *does not divide* a*.*

Proof. If we make the induction hypothesis

$$\mathcal{P}(k) \iff \forall (a_1, a_2, \ldots, a_k) \in \mathbb{Z}^k,\ (a_1 + a_2 + \cdots + a_k)^p \equiv a_1^p + a_2^p + \cdots + a_k^p$$

(which is true for $k = 1, k = 2$) then, from induction hypothesis and the case $k = 2$ already proved in Ex 3.12,

$$\begin{aligned}(a_1 + a_2 + \cdots + a_k + a_{k+1})^p &= ((a_1 + a_2 + \cdots + a_k) + a_{k+1})^p \\ &\equiv (a_1 + a_2 + \cdots + a_k)^p + a_{k+1}^p \pmod p \\ &\equiv a_1^p + a_2^p + \cdots + a_k^p + a_{k+1}^p \pmod p\end{aligned}$$

so $\mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)$:

$$\forall k \in \mathbb{N}^*, \forall (a_1, a_2, \ldots, a_k) \in \mathbb{Z}^k,\ (a_1 + a_2 + \cdots + a_k)^p \equiv a_1^p + a_2^p + \cdots + a_k^p.$$

If we apply this result to the particular case $a_1 = a_2 = \cdots = a_k = 1$, we obtain

$$\forall k \in \mathbb{N}^*,\ k^p \equiv k \pmod p.$$

and $(-k)^p \equiv -k^p \equiv -k \pmod p$ (even if $p = 2$), and $0^p = 0$, so

$$\forall k \in \mathbb{Z},\ k^p \equiv k \pmod p.$$

If $p \nmid a, a \in \mathbb{Z}$, then $p \wedge a = 1$, and $p \mid a^p - a = a(a^{p-1} - 1)$, so $p \mid a^{p-1} - 1, a^{p-1} \equiv 1 \pmod p$: this is another proof of Fermat's theorem. □

Ex. 3.14 *Let p and q be distinct odd primes such that $p-1$ divides $q-1$. If $(n, pq) = 1$, show that $n^{q-1} \equiv 1 \pmod{pq}$.*

Proof. As $n \wedge pq = 1, n \wedge p = 1, n \wedge q = 1$, so from Fermat's Little Theorem

$$n^{q-1} \equiv 1 \pmod{q}, \qquad n^{p-1} \equiv 1 \pmod{p}.$$

$p - 1 \mid q - 1$, so there exists $k \in \mathbb{Z}$ such that $q - 1 = k(p - 1)$. Thus

$$n^{q-1} = (n^{p-1})^k \equiv 1 \pmod{p}.$$

$p \mid n^{q-1} - 1, q \mid n^{q-1} - 1$, and $p \wedge q = 1$, so $pq \mid n^{q-1} - 1$:

$$n^{q-1} \equiv 1 \pmod{pq}.$$

□

Ex. 3.15 *For any prime p show that the numerator of $1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1}$ is divisible by p.*

Proof. As the result is false for $p = 2$, we must suppose $p > 2$, so p is odd.
$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} = \frac{N}{D}$, where

$$N = (p-1)! + \frac{(p-1)!}{2} + \cdots + \frac{(p-1)!}{p-1}, \qquad D = (p-1)!.$$

From Wilson's theorem, $(p-1)! \equiv -1 \pmod{p}$, so in the field $\mathbb{Z}/p\mathbb{Z}$,

$$\overline{N} = (-\overline{1})(\overline{1}^{-1} + \overline{2}^{-1} + \cdots + \overline{p-1}^{-1}).$$

As the application $\varphi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*, x \mapsto x^{-1}$ is bijective (it's an involution),

$$\overline{1} + \overline{2}^{-1} + \cdots + \overline{p-1}^{-1} = \overline{1} + \overline{2} + \cdots + \overline{p-1} = \overline{p} \times \overline{\left(\frac{p-1}{2}\right)} = \overline{0}.$$

So $p \mid N$, and $p \wedge (p-1)! = 1$, that is $p \wedge D = 1$. Thus p divides the numerator of the reduced fraction of N/D. □

Ex. 3.16 *Use the proof of the Chinese Remainder Theorem to solve the system $x \equiv 1 \pmod{7}$, $x \equiv 4 \pmod{9}$, $x \equiv 3 \pmod{5}$.*

Proof. Let $m_1 = 7, m_2 = 9, m_3 = 5, m = m_1 m_2 m_3 = 315, n_1 = m/m_1 = m_2 m_3 = 45, n_2 = m_1 m_3 = 35, n_3 = m_1 m_2 = 63$.
If $r_1 = 13, s_1 = -2$, then $r_1 m_1 + s_1 n_1 = 13 m_1 - 2 m_2 m_3 = 13 \times 7 - 2 \times 45 = 1$,
so $e_1 = s_1 n_1 = -2 \times 45 = -90$ verifies

$$e_1 = -90, \qquad e_1 \equiv 1 \pmod{7}, e_1 \equiv 0 \pmod{9}, e_1 \equiv 0 \pmod{5}.$$

If $r_2 = 4, s_2 = -1$, then $r_2 m_2 + s_2 n_2 = 4 \times 9 - 1 \times 35 = 1$,
so $e_2 = s_2 n_2 = -35$ verifies

$$e_2 = -35, \qquad e_2 \equiv 0 \pmod{7}, e_2 \equiv 1 \pmod{9}, e_2 \equiv 0 \pmod{5}.$$

If $r_3 = -25, s_3 = 2$, then $r_3 m_3 + s_3 n_3 = -25 \times 5 + 2 \times 63 = 1$, so $e_3 = s_3 n_3 = 2 \times 63 = 126$ verifies

$$e_3 = 126, \qquad e_3 \equiv 0 \pmod 7, e_3 \equiv 0 \pmod 9, e_3 \equiv 1 \pmod 5.$$

Let $x_0 = e_1 + 4e_2 + 3e_3 = 148$: then

$$x_0 = 148, \qquad x_0 \equiv 1 \pmod 7, x_0 \equiv 4 \pmod 9, x_0 \equiv 3 \pmod 5.$$

If $x \in \mathbb{Z}$ is any solution of the system, then $7 \mid x - x_0, 9 \mid x - x_0, 5 \mid x - x_0$, with $7 \wedge 9 = 7 \wedge 5 = 9 \wedge 5 = 1$, so $m = 315 \mid x - x_0$:

$$x = 148 + k\,315, k \in \mathbb{Z},$$

and all these integers are solutions of the system. $\square$

Ex. 3.17 *Let $f(x) \in \mathbb{Z}[x]$ and $n = p_1^{a_1} \cdots p_t^{a_t}$. Show that $f(x) \equiv 0 \pmod n$ has a solution iff $f(x) \equiv 0 \pmod{p_i^{a_i}}$ has a solution for $i = 1, \ldots, t$.*

Proof. If x is such that $f(x) \equiv 0 \pmod n$, as $p_i^{\alpha_i} \mid n$, $f(x) \equiv 0 \pmod{p_i^{a_i}}$.

Reciprocally, let $x_1, x_2, \ldots, x_t$ such that

$$\begin{gathered} f(x_1) \equiv 0 \pmod{p_1^{a_1}} \\ \cdots \\ f(x_t) \equiv 0 \pmod{p_t^{a_t}} \end{gathered}$$

As $p_i^{a_i} \wedge p_j^{a_j} = 1$ if $i \neq j$, the Chinese Remainder Theorem gives an integer x such that $x \equiv x_i \pmod{p_i^{a_i}}$, $i = 1, 2, \ldots, t$. As $f(x) \in \mathbb{Z}[x]$, $f(x) \equiv f(x_i) \equiv 0 \pmod{p_i^{a_i}}$. So $p_i^{a_i} \mid f(x)$, $i = 1, 2, \ldots, t$, where $p_i^{a_i} \wedge p_j^{a_j} = 1$ if $i \neq j$, then $n = p_1^{a_1} \cdots p_t^{a_t} \mid f(x)$: x is a somution of $f(x) \equiv 0 \pmod n$.

Conclusion : $f(x) \equiv 0 \pmod n$ has a solution iff $f(x) \equiv 0 \pmod{p_i^{a_i}}$ has a solution for $i = 1, \ldots, t$. $\square$

Ex. 3.18 *For $f \in \mathbb{Z}[x]$, let N be the number of solutions to $f(x) \equiv 0 \pmod n$ and N_i be the number of solutions to $f(x) \equiv 0 \pmod{p_i^{a_i}}$. Prove that $N = N_1 N_2 \cdots N_t$.*

Proof. Note $[x]_n$ the class of x modulo n. Let S the set of solutions in $\mathbb{Z}/n\mathbb{Z}$ of $f(\overline{x}) = 0$, and S_i the set of solutions in $\mathbb{Z}/p^{a_i}\mathbb{Z}$ of $f(\overline{x}) = 0$.

(We designate with the same letter the polynomial f in $\mathbb{Z}[x]$ or its reduction in $\mathbb{Z}/n\mathbb{Z}[x]$.)

Let

$$\varphi : \left\{ \begin{array}{ccc} S & \to & S_1 \times S_2 \times \cdots \times S_t \\ [x]_n & \mapsto & ([x]_{p_1^{a_1}}, [x]_{p_2^{a_2}}, \ldots, [x]_{p_t^{a_t}}) \end{array} \right.$$

- φ is well defined : if $x \equiv x' \pmod n$, then $x \equiv x' \pmod{p_i^{a_i}}$, $i = 1, 2, \cdots, t$, so $([x]_{p_1^{a_1}}, [x]_{p_2^{a_2}}, \ldots, [x]_{p_t^{a_t}}) = ([x']_{p_1^{a_1}}, [x']_{p_2^{a_2}}, \ldots, [x']_{p_t^{a_t}})$. Moreover, we proved in Ex 3.17 that $[x]_n \in S \Rightarrow [x]_{p_i^{a_i}} \in S_i$.
- φ is injective : if $([x]_{p_1^{a_1}}, [x]_{p_2^{a_2}}, \ldots, [x]_{p_t^{a_t}}) = ([x']_{p_1^{a_1}}, [x']_{p_2^{a_2}}, \ldots, [x']_{p_t^{a_t}})$, then $p_i^{a_i} \mid x' - x$, $i = 1, 2, \ldots, t$, so $n \mid x' - x$ and $[x]_n = [x']_n$.
- φ is surjective : if $y = ([x_1]_{p_1^{a_1}}, [x_2]_{p_2^{a_2}}, \ldots, [x_t]_{p_t^{a_t}})$ is any element of $S_1 \times S_2 \times \cdots \times S_t$, there exists from Chinese remainder theorem $x \in \mathbb{Z}$ such that $x \equiv x_i \pmod{p_i^{a_i}}$. Then $\varphi([x]_n) = y$ (see Ex. 3.17).

In conclusion, a φ is bijective, $N = |S| = |S_1 \times S_2 \times \cdots \times S_t| = N_1 N_2 \cdots N_t$. $\square$

Ex. 3.19 *If p is an odd prime, show that 1 and -1 are the only solutions of $x^2 \equiv 1 \pmod{p^a}$.*

Proof.

$$x^2 - 1 \pmod{p^a} \iff p^a \mid (x-1)(x+1).$$

Let $d = (x-1) \wedge (x+1)$: $d = 1$ or $d = 2$.

• If $d = 1$, then x is even (if not, $x-1$ and $x+1$ are even, and $2 \mid d$). As $p^a \mid (x-1)(x+1)$ and $(x-1) \wedge (x+1) = 1$, then $p^a \mid x-1$, or $p^a \mid x+1$, that is

$$x \equiv \pm 1 \pmod{p^a}.$$

• If $d = 2$, then x is odd, and

$$p^a \mid 4 \frac{x-1}{2} \frac{x+1}{2}.$$

As p is an odd prime, $p \wedge 4 = 1$, so $p \mid \frac{x-1}{2}\frac{x+1}{2}$, where $\frac{x-1}{2} \wedge \frac{x+1}{2} = 1$, hence $p^a \mid \frac{x-1}{2} \mid x-1$ or $p^a \mid \frac{x+1}{2} \mid x+1$:

$$x \equiv \pm 1 \pmod{p^a}.$$

$\{-\overline{1}, \overline{1}\}$ is the set of roots of $x^2 - \overline{1}$ in $\mathbb{Z}/p^a\mathbb{Z}$. □

Ex. 3.20 *Show that $x^2 \equiv 1 \pmod{2^b}$ has one solution if $b = 1$, two solutions if $b = 2$, and four solutions if $b \geq 3$.*

Proof. Consider the equation $x^2 \equiv 1 \pmod{2^b}$.

• If $b = 1$, $x^2 \equiv 1 \pmod 2 \iff 2 \mid (x-1)(x+1) \iff x \equiv 1 \pmod 2$: one solution.

• If $b = 2$, as $0^2 \equiv 2^2 \equiv 0 \pmod 4$, $x^2 \equiv 1 \pmod 4 \iff x \equiv \pm 1 \pmod 4$: two solutions.

• Suppose $b \geq 3$. The equation has 4 solutions $1, -1, 1 + 2^{b-1}, -1 + 2^{b-1}$.

Indeed, $(\pm 1)^2 \equiv 1 \pmod{2^b}$, and

$$(1 + 2^{b-1})^2 = 1 + 2.2^{b-1} + 2^{2b-2} = 1 + 2^b(1 + 2^{b-2}) \equiv 1 \pmod{2^b},$$

and similarly $(-1 + 2^{b-1})^2 \equiv 1 \pmod{2^b}$.

These solutions are incongruent modulo 2^b :

$1 \not\equiv -1 \pmod{2^b}$ and $1 + 2^{b-1} \not\equiv -1 + 2^{b-1}$ (if not, $2^b \mid 2$, so $b \leq 1$).

$1 + 2^{b-1} \equiv -1 \pmod{2^b} \iff 2^b \mid 2 + 2^{b-1} = 2(1 + 2^{b-2})$: so $2 \mid 2^{b-1} \mid (1 + 2^{b-2})$, this is impossible because $1 + 2^{b-2}$ is odd ($b \geq 3$). With the same argument, $-1 + 2^{b-1} \not\equiv 1 \pmod{2^b}$. $1 + 2^{b-1} \equiv 1 \pmod{2^b}$ implies $2^b \mid 2^{b-1}$, so $2 \mid 1$: this is a contradiction, so $1 + 2^{b-1} \not\equiv 1 \pmod{2^b}$, and also $-1 + 2^{b-1} \not\equiv -1 \pmod{2^b}$. There exist at least 4 solutions.

We show that these are the only solutions :

$$\forall x \in \mathbb{Z},\ x^2 \equiv 1 \pmod{2^b} \Rightarrow x \equiv \pm 1 \pmod{2^{b-1}}.$$

Indeed, if $x^2 \equiv 1 \pmod{2^b}$, $2^b \mid (x-1)(x+1)$, where $d = (x-1) \wedge (x+1) = 2$.

As in Ex.3.19, if $d = 1$, then $2^b \mid x-1$ or $2^b \mid x+1$, a fortiori $x \equiv \pm 1 \pmod{2^{b-1}}$.

If $d = 2$, then x is odd, and $2^b \mid 4\frac{x-1}{2}\frac{x+1}{2}$, so $2^{b-2} \mid \frac{x-1}{2}\frac{x+1}{2}$, with $\frac{x-1}{2} \wedge \frac{x+1}{2} = 1$, so $2^{b-2} \mid \frac{x-1}{2}$ or $2^{b-2} \mid \frac{x+1}{2}$, that is $2^{b-1} \mid x-1$ or $2^{b-1} \mid x+1$: $x \equiv \pm 1 \pmod{2^{b-1}}$.

(Alternatively, we can prove this implication by induction.)

Hence every solution of $x^2 \equiv 1 \pmod{2^b}, b \geq 3$ is such that $x = \pm 1 + k2^{b-1}, k \in \mathbb{Z}$: there exit only four such value in the interval $[0, 2^b[$, namely $1, -1+2^b-1, 1+2^{b-1}, -1+2^b$.

Conclusion : if $b \geq 3$, the roots of $x^2 - 1$ in $\mathbb{Z}/2^b\mathbb{Z}$ are $\overline{1}, -\overline{1}, \overline{1} + \overline{2}^{b-1}, -\overline{1} + \overline{2}^{b-1}$. □

Ex. 3.21 *Use Ex. 18-20 to find the number of solutions to $x^2 \equiv 1 \pmod n$.*

Proof. Let $n = 2^{a_0} p_1^{a_1} \cdots p_k^{a_k}$ the decomposition in prime factors of $n > 1$ ($p_0 = 2 < p_1 < \cdots < p_k, a_0 \geq 0, a_i > 0, 1 \leq i \leq k$). Let N the number of solutions of $x^2 \equiv 1 \pmod n$, and N_i the number of solutions of $x^2 \equiv 1 \pmod{p^i}, i = 0, 1, \ldots k$. From Ex.3.18, we know that $N = N_0 N_1 \cdots N_k$, where (Ex. 3.19), $N_i = 2, i = 1, 2, \ldots, k$, and (Ex.3.20), $N_0 = 1$ if $a_0 = 1$ (or $a_0 = 0$), $N_0 = 2$ if $a_0 = 2$, $N_0 = 4$ if $a_0 \geq 3$.

Conclusion : the number of solutions of $x^2 \equiv 1 \pmod n$, where $n = 2^{a_0} p_1^{a_1} \cdots p_k^{a_k}$, is

$$\begin{aligned} N &= 2^k \quad \text{if } a_0 = 0 \text{ or } a_0 = 1 \\ N &= 2^{k+1} \quad \text{if } a_0 = 2 \\ N &= 2^{k+2} \quad \text{if } a_0 \geq 3 \end{aligned}$$

□

Ex. 3.22 *Formulate and prove the Chinese Remainder Theorem in a principal ideal domain.*

Proposition. *Let R a principal ideal domain, and $m_1, \ldots, m_t \in R$. Suppose that $(m_i, m_j) = 1$ for $i \neq j$ (that is $(m_i) + (m_j) = (1), m_i R + n_i R = R$). Let $b_1, \ldots, b_t \in R$ and consider the system of congruences:*

$$x \equiv b_1 \pmod{m_1}, x \equiv b_2 \pmod{m_2}, \ldots, x \equiv b_t \pmod{m_t}.$$

This system has solutions and any two solutions differ by a multiple of $m_1 m_2 \cdots m_t$.

Proof. Let $m = m_1 m_2 \cdots m_t$, and $n_i = m/m_i,\ i = 1, 2, \ldots, t$.

As $(m_1, m_i) = (1)$, we can find $u_i, v_i \in R$ such that $m_1 u_i + m_i v_i = 1,\ i = 2, \ldots, t$.

So $1 = \prod_{i=2}^{t} (m_1 u_i + m_i v_i) = m_1 u + (m_2 \cdots m_t) v$ for some elements $u, v \in R$, thus $(m_1, n_1) = (m_1, m_2 m_3 \cdots m_t) = (1)$, and similarly $(m_i, n_i) = 1$. So there are $r_i, s_i \in R$ such that $r_i m_i + s_i n_i = 1$. Let $e_i = s_i n_i$. Then $e_i \equiv 1 \pmod{m_i}$ and $e_i \equiv 0 \pmod{m_j}$ for $j \neq i$.

Set $x_0 = \sum_{i=1}^{t} b_i e_i$. Then we have $x_0 \equiv b_i e_i \equiv b_i \pmod{m_i}$ and so x_0 is a solution.

Suppose that x_1 is another solution. Then $x_1 - x_0 \equiv 0 \pmod{m_i}$ for $i = 1, 2, \ldots, t$, in other words $m_1, m_2, \ldots, m_t$ divide $x_1 - x_0$, with $(m_i, m_j) = 1$: from lemma 2 generalized to principal rings, m divides $x_1 - x_0$. □

This result can be generalized to any commutative ring, not necessarily a PID (see S.LANG, Algebra):

Proposition. *Let A a commutative ring. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals of A such that $\mathfrak{a}_i + \mathfrak{a}_j = A$ for all $i \neq j$. Given elements $x_1, \ldots, x_n \in A$, there exists $x \in A$ such that $x \equiv x_i \pmod{\mathfrak{a}_i}$ for all i.*

Ex. 3.23 *Extend the notion of congruence to the ring $\mathbb{Z}[i]$ and prove that $a + bi$ is always congruent to 0 or 1 modulo $1 + i$.*

Proof. If a, b, c are in $\mathbb{Z}[i]$ we say that $a \equiv b \pmod c$ if there exists $q \in \mathbb{Z}[i]$ such that $a - b = qc$.

As $i \equiv -1 \pmod{1 + i}, a + bi \equiv a - b \pmod{1 + i}$.

$(1 - i)(1 + i) = 2$, so $2 \equiv 0 \pmod{1 + i}$.

If $a-b$ is even, $a-b=2k, k\in\mathbb{Z}\subset\mathbb{Z}[i]$, so $a-b\equiv 0 \pmod{1+i}$.
If $a-b$ is odd, $a-b=2k+1, k\in\mathbb{Z}$, so $a-b\equiv 1 \pmod{1+i}$.
Conclusion : for all $z\in\mathbb{Z}[i]$, $z\equiv 0,1 \pmod{1+i}$. ☐

Ex. 3.24 *Extend the notion of congruence to the ring $\mathbb{Z}[\omega]$ and prove that $a+b\omega$ is always congruent to -1, 0 or 1 modulo $1-\omega$.*

Proof. Same definition of congrence in $\mathbb{Z}[\omega]$ as in Ex. 3.23.
$\omega\equiv 1 \pmod{1-\omega}$, so $a+b\omega\equiv a+b \pmod{-\omega}$.
$0=1-\omega^3=(1-\omega)(1+\omega+\omega^2)$, with $1-\omega\neq 0$, so $1+\omega+\omega^2=0$. Hence $3\equiv 0 \pmod{1-\omega}$.
$a+b\equiv 0,1,-1 \pmod 3$, so $a+b\equiv 0,1,-1 \pmod{1-\omega}$
For all $z\in\mathbb{Z}[\omega]$, $z\equiv 0,1,-1 \pmod{1-\omega}$. ☐

Ex. 3.25 *Let $\lambda=1-\omega\in\mathbb{Z}[\omega]$. If $\alpha\in\mathbb{Z}[\omega]$ and $\alpha\equiv 1 \pmod\lambda$, prove that $\alpha^3\equiv 1 \pmod 9$.*

Proof. $\alpha\equiv 1 \pmod\lambda$, so $\alpha=1+\beta\lambda, \beta\in\mathbb{Z}[\omega]$.
$\overline{\lambda}=1-\omega^2=(1-\omega)(1+\omega)=-\omega^2(1-\omega)=-\omega^2\lambda$ (so $\overline{\lambda}$ and λ are associate).

$$\begin{aligned}\alpha^3-1&=(\alpha-1)(\alpha-\omega)(\alpha-\omega^2)\\&=(\alpha-1)(\alpha-1+\lambda)(\alpha-1+\overline{\lambda})\\&=(\alpha-1)(\alpha-1+\lambda)(\alpha-1-\omega^2\lambda)\\&=\beta\lambda(\beta\lambda+\lambda)(\beta\lambda-\omega^2\lambda)\\&=\lambda^3\beta(\beta+1)(\beta-\omega^2)\end{aligned}$$

Moreover,

$$\begin{aligned}\beta(\beta+1)(\beta-\omega^2)&\equiv\beta(\beta+1)(\beta-1)\pmod\lambda\\&\equiv 0\pmod\lambda\end{aligned}$$

since $\beta\equiv 0,1,-1 \pmod\lambda$ (see Ex. 3.24).
So $\lambda^4\mid\alpha^3-1$.
As $\lambda\overline{\lambda}=(1-\omega)(1-\omega^2)=1-\omega-\omega^2+\omega^3=3$, then $\lambda\overline{\lambda}=-\omega^2\lambda^2=3$, so λ^2 and 3 are associate : $\lambda^2=-\omega\lambda^2$. So $9=(-\omega^2\lambda^2)^2=\omega\lambda^4$, so $9\mid\omega^2 9=\lambda^4\mid\alpha^3-1$.
For all $\alpha\in\mathbb{Z}[\omega]$,

$$\alpha\equiv 1 \pmod\lambda\Rightarrow\alpha^3\equiv 1 \pmod 9.$$

☐

Ex. 3.26 *Use Ex. 25 to show that ξ,η,ζ are not zero and $\xi^3+\eta^3+\zeta^3=0$, then λ divides at least one of the elements ξ,η,ζ.*

Proof. Let $\xi,\eta,\zeta\in\mathbb{Z}[\omega]\setminus\{0\}$ such that $\xi^3+\eta^3+\zeta^3=0$.
With a reductio ad absurdum, suppose that $\lambda\nmid\xi,\lambda\nmid\eta,\lambda\nmid\zeta$.
From Ex. 3.24,

$$\xi\equiv\pm1\pmod\lambda,\eta\equiv\pm1\pmod\lambda,\zeta\equiv\pm1\pmod\lambda,$$

and from Ex.3.25,

$$\xi^3 \equiv \pm 1 \pmod 9, \eta^3 \equiv \pm 1 \pmod 9, \zeta^3 \equiv \pm 1 \pmod 9,$$

As $\pm 1 \pm 1 \pm 1 \not\equiv 0 \pmod 9$, this is a contradiction.

Conclusion : if ξ, η, ζ are not zero and $\xi^3 + \eta^3 + \zeta^3 = 0$, then λ divides at least one of the elements ξ, η, ζ.

(consequence : if $x^3 + y^3 + z^3 = 0,\ x, y, z \in \mathbb{Z}$, then $3 \mid xyz$: this is the first case of Fermat's theorem for the exponant 3.) $\square$

4 Chapter 4

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

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

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

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

$2^{28} \equiv 1[29]$ and $2^d \not\equiv 1$ if $d \mid 28, d < 28$, 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 $2, 2^3, 2^7, 2^9$.

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

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

Similarly :

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

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

• $p = 19 : \{2, 13, 14, 15, 3, 10\}$ 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])
```

$\square$

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 $\overline{a}$ is a generator of $U(\mathbb{Z}/p^n\mathbb{Z})$.

If a was not a primitive root modulo p, $\overline{a}$ 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 $\overline{b} \in U(\mathbb{Z}/p^n\mathbb{Z})$ and $\overline{b} \notin \langle \overline{a} \rangle$ 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.) $\square$

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.

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

If n is odd, then $a^n \equiv -1, a^{2n} \equiv 1 \pmod{p}$. As a is a primitive root modulo p, $p-1 \mid 2n$, $2t \mid n$, so n is even : this is a contradiction.

Consequently, n is even, and $a^n \equiv 1 \pmod{p}$, so $p-1 \mid n$, 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.

Reciprocally, if $-a$ is a primitive root modulo p, we apply the previous result at $-a$ to 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 $i = 1, 2, \cdots k$, $(p-1)/p_i$ 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. □

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.

Reciprocally, suppose that $-a$ has order $(p-1)/2 = 2t+1$ modulo p. Let $2, p_1, \ldots p_k$ 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 $a^{(p-1)/2} \not\equiv 1 \pmod{2}$.

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. □

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 :

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

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 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 $2u \equiv -1 + a \pmod p$ ($\overline{u}$ 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 $\overline{u}$ 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 $p = 2^{2^n} + 1$. ☐

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 suffisant 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 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 $p^2 \equiv 1 \pmod{16}$, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = -1$, 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. □

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 $\delta \mid p-1, \delta = q_1^{b_1} p_2^{b_2} \cdots q_k^{b_k}$, with $b_i \leq a_i, i = 1, 2, \ldots, k$. 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. □

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 $\overline{g}$:

$$U(\mathbb{Z}/p\mathbb{Z}) = \{\overline{1}, \overline{g}, \overline{g}^2, \ldots, \overline{g}^{p-2}\}, \qquad \overline{g}^{p-1} = \overline{1}.$$

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

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

so $\overline{P} = \overline{g}^S$, 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. $(\overline{g}^{(p-1)/2})^2 = \overline{g}^{p-1} = \overline{1}$, and $\overline{g}^{(p-1)/2} \neq \overline{1}$. As $\mathbb{Z}/p\mathbb{Z}$ is a field, $\overline{g}^{(p-1)/2} = -\overline{1}$.

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

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

□

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 $x \in \mathbb{F}_p^*$, $\mathbb{N}^* = \{1, 2, 3, \ldots\}$.

Let

$$\psi : \left\{ \begin{array}{ccc} \mathbb{N}^* & \to & \mathbb{F}_p \\ n & \mapsto & \psi(n) = \sum\limits_{d \in \mathbb{F}_p^*, |d| = n} d \end{array} \right.$$

$\psi(n)$ 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 $n \in \mathbb{N}^*$

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

$f(n)$ is the sum of elements whose order divides n, in other worlds 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

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

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

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

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

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. □

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

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

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

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

$$\begin{aligned} \overline{S_k} &= \overline{1}^k + \overline{2}^k + \cdots + \overline{p-1}^k \\ &= \sum_{i=0}^{p-2} \overline{g}^{ki} = \left\{ \begin{array}{lll} \overline{p-1} = -\overline{1} & \text{if} & p-1 \mid k \\ \frac{\overline{g}^{(p-1)k} - 1}{\overline{g}^k - 1} = \overline{0} & \text{if} & p-1 \nmid k \end{array} \right. \end{aligned}$$

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

Conclusion :

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

□

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 : $\overline{g}$ a generator of $\mathbb{F}_p^*$.

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

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

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 $\operatorname{Card} G = n$, 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 $n \wedge k = 1$.

Reciprocally, 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 $m \wedge k$.

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

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

• Reciprocally, if $nm \mid k, nm = qnm, q \in \mathbb{Z}$, 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 $\sum_{c|d} \psi(c) = d$. Applying the Möbius inversion theorem, $\psi(d) = \sum_{c|d} \mu(c) d/c = \Phi(d)$ (Prop. 2.2.5), in particular, $\psi(n) = \phi(n) > 1$ if $n > 2$. Since a group of order 2 is cyclic, we have shown in all cases 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 $\psi(d) \le \phi(d)$ for all $d \mid n$. As $\sum_{d|n} \psi(d) = \sum_{d|n} \phi(d) = n$, $\psi(d) = \phi(d)$ for all $d \mid n$. So there exists in G an element of order n, and G is cyclic.) □

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 $a^{n/p_1} \ne 1$.

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 $c_1^{p_1^{a_1 - 1}} = a^{n/p_1} \ne 1$, so $|c_1| = p_1^{a_1}$.

Similarly, there exist $c_2, \ldots, c_k$ 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. □

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 a in $\mathbb{Z}/p\mathbb{Z}$.

Let $x \in \mathbb{F}_{19}$. $x^3 - 1 = 0 \iff x - 1 = 0$ or $x^2 + x + 1 = 0$.

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

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

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

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

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

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 $x = 2^k \in \mathbb{F}_{19}$.

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

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

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

□

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

$$S = \{1, 2^4, 2^8, 2^{12}, 2^{16}, 2^{20}, 2^{24}\},$$

$$S = \{1, 16, 24, 7, 25, 23, 20\}.$$

□

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

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

$$1 + x + \cdots + x^6 \equiv 0 \pmod{29} \iff \left\{ \begin{array}{rcll} x^7 & \equiv & 1 & \pmod{29} \\ x & \not\equiv & 1 & \pmod{29} \end{array} \right.$$

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

$$f : \left\{ \begin{array}{ccc} \mathbb{F}_{11}^* & \to & \mathbb{F}_{11}^* \\ x & \mapsto & x^3 \end{array} \right.$$

f is a bijection. Indeed,

- f is a group homomorphism,
- $x^3 = 1 \Rightarrow (x^3)^7 = 1 \Rightarrow x = 1$ so $\ker(f) = \{1\}$,
- $f : \mathbb{F}_{11}^* \to \mathbb{F}_{11}^*$ 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 dth 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

$$f : \left\{ \begin{array}{ccc} \mathbb{F}_p^* & \to & \mathbb{F}_p^* \\ x & \to & x^d \end{array} \right.$$

Then f is a group homomorphism, and $\mathrm{im}(f)$ is the set of dth 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 $\mathrm{im}(f) \simeq \mathbb{F}_p^*/\ker(f)$,

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

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

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

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

So the group of dth powers is the group of the roots of $x^{(p-1)/d} - 1$.
- If $p = 11, d = 5$, $\mathrm{im}(f) = \{1, -1\}$.
- If $p = 17, d = 4$, $x \in \mathrm{im}(f) \iff x^4 = 1 : \mathrm{im}(f) = \{1, -1, 4, -4\}$.
- If $p = 19, d = 6$, $x \in \mathrm{im}(f) \iff x^3 = 1 : \mathrm{im}(f) = \{1, 7, 7^2 = 11\}$,

where $7 \equiv 2^6 \pmod{19}$.

□

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

Proof. Let $x = \overline{g}^{(p-1)/d} \in \mathbb{F}_p^*$, 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 ordre of $\overline{g}^{(p-1)/d}$ is d.

- If $\overline{a} = \overline{g}^{kd}$, then $\overline{a} = x^d$, where $x = \overline{g}^k$, so $\overline{a}$ is a dth power.
- If $\overline{a} \neq \overline{0}$ is a dth power, $\overline{a} = x^d, x \in \mathbb{F}_p^*$. As $x \in \langle \overline{g} \rangle$, $x = \overline{g}^k$, so $\overline{a} = \overline{g}^{kd}$.

So, if $a \not\equiv 0 \pmod p$, a is a dth 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 $2^0 = 1, 2^6 = 7, 2^{12} = 11$. □

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 divides 2 or 3, so $1+a$ has order 6 modulo p. □

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 $\overline{x}$ has order 4 in $\mathbb{F}_p^*$, hence from Lagrange's theorem, $4 \mid p-1$.

Reciprocally, 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 $\overline{x}^8 = 1 \in \mathbb{F}_p^*$, and $\overline{x}^4 \neq 1$, so x has order 8 in $\mathbb{F}_p^*$, so $8 \mid p-1$.

Reciprocally, 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 :

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

□

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 $(\overline{x}, \overline{y})$ of the equation $\overline{a}\,\overline{x}^m + \overline{b}\,\overline{y}^n = \overline{c}$,$N'$ the number of solutions $(\overline{x}, \overline{y})$ of the equation $\overline{a}\,\overline{x}^{m'} + \overline{b}\,\overline{y}^{n'} = \overline{c}$. Then

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

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

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

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

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

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

So

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

and similarly

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

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 $\overline{u}$.

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

Write $\overline{x} = \overline{g}^k, \overline{x_0} = g^{k_0}$. Let $d = m \wedge (p-1) (= m')$.

$$\begin{aligned}
\overline{x}^m = u &\iff \overline{x}^m = \overline{x_0}^m\\
&\iff \overline{g}^{mk} = \overline{g}^{mk_0}\\
&\iff p-1 \mid m(k-k_0)\\
&\iff \frac{p-1}{d} \mid \frac{m}{d}(k-k_0)\\
&\iff \frac{p-1}{d} \mid k-k_0\\
&\iff \exists j \in \mathbb{Z}, k = k_0 + j\frac{p-1}{d}
\end{aligned}$$

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

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

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

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

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 $5^{nz} \equiv 5^t \pmod{2^e}$.

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

$$x^n \equiv a \pmod{2^e} \iff \left\{ \begin{array}{lll} ny & \equiv & s \pmod 2 \\ 5^{nz} & \equiv & 5^t \pmod{2^e} \end{array} \right. \iff \left\{ \begin{array}{lll} ny & \equiv & s \pmod 2 \\ nz & \equiv & t \pmod{2^{e-2}} \end{array} \right.$$

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

• Suppose that n is an odd integer. Then

$$\left\{ \begin{array}{lll} ny & \equiv & s \pmod 2 \\ nz & \equiv & t \pmod{2^{e-2}} \end{array} \right. \iff \left\{ \begin{array}{lll} y & \equiv & s \pmod 2 \\ z & \equiv & n't \pmod{2^{e-2}} \end{array} \right.$$

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 $\left\{ \begin{array}{lll} ny & \equiv & s \pmod 2 \\ nz & \equiv & t \pmod{2^{e-2}} \end{array} \right.$ 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 $d = n \wedge 2^{e-2}$,

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

Reciprocally, suppose that $\left\{\begin{array}{lcl} a & \equiv & 1 \pmod 4 \\ a^{\frac{2^{e-2}}{d}} & \equiv & 1 \pmod{2^e} \end{array}\right.$. 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 $d \mid t$.

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

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

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

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

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

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

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

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 $e \ge 2l + 1$, and consequently for all $e \ge 1$). 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 $m \ge 2l + 1$,

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

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

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

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

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

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

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 an 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 $x_1^b \equiv a \pmod{2^{m+1}}$, 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 $l = \mathrm{ord}_2(n)$, 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 $e \geq 2l+1, e \geq 3$. $\square$