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

Richard Ganaye

September 1, 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 $\mathbb{N} = \{0, 1, 2, \cdots\}$ 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
```

$\square$

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

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

We show by induction on i $(i \le k+1)$ 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)
```

□

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 :

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

□

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 $a' \wedge b' = 1$.

□

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 $m \leq n$.

In this case $1/m \geq 1/n$, so $2/n \leq 1/2 : n \geq 4$.

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

If $m = 1$, $n < 0 :$ it is impossible. If $m = 2$, $1/n = 0 :$ also impossible. Therefore $n \leq 6 : 4 \leq n \leq 5$. 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. ☐

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

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

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

We define

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

The characterization of the gcd is

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

$$(i)\ d \geq 0 \tag{3}$$

$$(ii)\ d \mid n_1, \cdots, d \mid n_s \tag{4}$$

$$(iii)\ \forall \delta \in \mathbb{Z},\ (\delta \mid n_1, \cdots, \delta \mid n_s) \Rightarrow \delta \mid d \tag{5}$$

($\Rightarrow$) Indeed, if we suppose (1), then $d \geq 0$, 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 $d \mid n_i, 1 \leq i \leq s$ so (i)(ii) are true. if $\delta \mid n_i, 1 \leq i \leq s$, as $d = n_1m_1 + \cdots + n_sm_s, m_1, \cdots, m_s \in \mathbb{Z}$, then $\delta \mid d$.

($\Leftarrow$)Suppose that d verify (i)(ii)(iii). From (ii), we see that $n_i\mathbb{Z} \subset d\mathbb{Z}, i = 1, \cdots, s$, 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 $n_i \in \delta\mathbb{Z},\ i = 1, \cdots, s : \delta \mid n_1, \cdots, \delta \mid n_s$. 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 $d = \gcd(n_1, \cdots, n_s)$.

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

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 $a_1, a_2, \cdots, a_r \in \mathbb{Z}$.

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

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

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 $d \mid a_1, \cdots, d \mid a_r$, $d \mid a_1x_1 + a_2x_2 + \cdots + a_rx_r = c$.
- 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 $d = a_1m_1 + a_2m_2 + \cdots + a_rm_r,\ m_1, m_2, \cdots, m_r \in \mathbb{Z}$. $c = dc' = a_1(m_1c') + \cdots a_r(m_rc') = a_1x_1 + \cdots + a_rx_r$, where $x_i = m_ic', i = 1, 2, \cdots, r$. □

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 $a \geq 0$. 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 $a \in \mathbb{Z}, a \geq 0$:

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

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 $\mathbb{N} = \{0, 1, 2, \cdots\}$.

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. □

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 $m = a \wedge b$. $\square$

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 $\mu = \varepsilon'' \prod\limits_p p^{c(p)}$ 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 exists 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

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

$\square$

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 : $S = \{P_1, P_2, \cdots, P_n\}$.

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 $p_1, p_2, \cdots, p_t \in \mathbb{Z}$ 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 $i = 1, 2, \cdots, t$. Show that this set is a ring and that up to taking associates $p_1, p_2, \cdots, p_t$ 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 $\mathrm{ord}_{p_i} a = \mathrm{ord}_{p_i}(b),\ i = 1, \cdots, t$. 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 $rs = p_i u$, with b, d, e relatively prime with $p_1, \cdots, p_t$. Then $acf = p_i bde$. 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 $b \wedge p_1 \cdots p_r = 1$, $a = p_1^{k_1} \cdots p_t^{k_t} v, v \in \mathbb{Z}, k_i \geq 0, i = 1, \cdots, t$. 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 $i = 1, \cdots, t$. Moreover $p_i \mid p$, so p_i and π are associate.

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

Ex. 2.3 *Use the formula for $\phi(n)$ to give a proof that there are infinitely many primes.*
[Hint: If $p_1, p_2, \cdots, p_t$ 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 $k_i \geq 0, i = 1, \cdots t$. 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

$$\begin{aligned} a^{2^n} &\equiv -1 \pmod d \\ a^{2^m} &\equiv -1 \pmod d \end{aligned}$$

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., $\left\lfloor \frac{1}{2} \right\rfloor = 0$, $\lfloor 2 \rfloor = 2$, and $\left\lfloor 3 + \frac{1}{3} \right\rfloor = 3$. Prove* $\mathrm{ord}_p\, n! = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor \cdots$.

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 $\mathrm{ord}_p\, n! = \sum_{k=1}^{n} \mathrm{ord}_p\, k$. Thus

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

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* $\mathrm{ord}_p n! \leq n/(p-1)$ *and that* $\sqrt[n]{n!} \leq \prod_{p\leq n} p^{1/(p-1)}$.
(The original statement $\prod_{p|n} p^{1/(p-1)}$ *was modified.)*

Proof.

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

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,

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

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 $i \neq j,\ i, j = 1, \cdots, t$,

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

(by induction on the number of prime factors.)

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

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. □

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 $p_1, \cdots, p_l, q_1, \cdots q_r$ 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 suffisant 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 $n \geq 1$,

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

□

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,

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

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

□

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 $h(n) = \sum_{d|n} \mu(n/d) f(d)$ 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

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

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

Ex. 2.15 *Show that*

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

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

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

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

(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 $n \geq 1$,
$$n = \mathrm{Id}(n) = \sum_{d|n} \mu(n/d)\sigma(d).$$

□

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 $i = 1, 2, \cdots, r$: n is a 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 $p_i^j, j = 0, \cdots, k_i$ is odd, the number of terms $k_i + 1$ is odd, so k_i is even $(i = 2, \cdots, t)$. Thus n is a square, or twice a 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 $\alpha_i, \beta_i, \lambda_j, \mu_k \in \mathbb{N}^*,\ 1 \le i \le r, 1 \le j \le s, 1 \le k \le t$ (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 $\gamma_i = \min(\alpha_i, \beta_i), \delta_i = \max(\alpha_i, \beta_i)$ $(\gamma_i \ge 1, \delta_i \ge 1), 1 \le i \le r$. 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* $\prod_{d|n} d = n^{\nu(n)/2}$.

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 $d = p_j^i, i > 0, j = 1, \cdots t$,
$$\begin{aligned}\sum_{d|n} \wedge(d) &= \sum_{i=1}^{\alpha_1} \wedge(p_1^i) + \cdots + \sum_{i=1}^{\alpha_t} \wedge(p_t^i) \qquad = \alpha_1 \log p_1 + \cdots + \alpha_t \log p_t\\ &= \log n\end{aligned}$$

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 $S = \sum_{1 \le t \le n-1,\ t \wedge n = 1} t$.

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

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

Conclusion :

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

□

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 $[j]_n = [k]_n, [j]_m = [k]n$, 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 $\psi(p^t) = \sum_{k=0}^{p^{t-1}-1} \mathrm{Card}\, C_k$, 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 $\psi(p^t) = p^{t-1}\,\mathrm{Card}\, I_0 = p^{t-1}\psi(p)$:

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

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

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

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

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

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

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

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

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

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

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

(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 $\sum\limits_{f \in \mathcal{P}} q^{-2 \deg f}$, if $\sum\limits_{p \in \mathcal{M}} q^{-\deg p(x)}$ 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 $\lim\limits_{n \to \infty} \lambda(n) = \infty$.

Conclusion : $\sum\limits_{p \in \mathcal{M}} q^{-\deg p(x)}$ diverges. $\square$

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 $\sum\limits_{n=1}^{\infty} |f(n)| = 1/n^u$ 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 $S^* = \sum\limits_{n=1}^{\infty} |f(n)| < \infty$, and $S = \sum\limits_{n=1}^{\infty} f(n) \in \mathbb{C}$. For each prime number p, $\sum\limits_{k=1}^{\infty} |f(p^k)|$ converges (this sum is less than S^*), so $\sum\limits_{k=0}^{\infty} f(p^k)$ 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

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

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)

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

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

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

(b)

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

So

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

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

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

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 $p_1, p_2, \cdots p_l$ $(l = l(N))$ 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

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

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

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

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

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

$\square$