Notes for 13-20 December, 2021

0.1 A few problems/properties involving $[x]$

1. The power of 10 dividing $n!$ is $v_5(n!)$ for every n. In other words, we have a formula for the number of zeroes that $n!$ ends in.
This is obvious from de Polignac's formula because if 5^k and 2^l are the powers of 5 and 2 (respectively) dividing $n!$, then $k \leq l$.

2. *Show, for all $n \geq 1$, that*

$$[\sqrt{n} + \sqrt{n+1}] = [\sqrt{4n+1}] = [\sqrt{4n+2}] = \sqrt{4n+3}].$$

As $n < \sqrt{n(n+1)} < n+1$, we get

$$2n < 2\sqrt{(n(n+1)} = (\sqrt{n} + \sqrt{n+1})^2 - (2n+1) < 2(n+1).$$

Thus,

$$4n + 1 < (\sqrt{n} + \sqrt{n+1})^2 < 4n + 3.$$

Taking square roots,

$$\sqrt{4n+1} < \sqrt{n} + \sqrt{n+1} < \sqrt{4n+3}.$$

If $m = [\sqrt{4n+1}]$, we have $[\sqrt{4n+3}] < m+1$ because no perfect square can be either of the form $4n+2$ or of the form $4n+3$. Thus, we have the assertion.

5. For any positive integers $2 \leq d \leq n$, consider the base d expansion of n; say, $n = a_0 + a_1 d + \cdots + a_r d^r$ with $0 \leq a_i < d$. Then, for all $i \geq 0$,

$$a_i = [n/d^i] - d[n/d^{i+1}].$$

In particular, if $d = p$, a prime, the power of p dividing $n!$ equals $\frac{n - \sum_{i=0}^{r} a_i}{p-1}$.
Thus, we may determine the power of a prime dividing $n!$ in terms of the sum of the base p digits of n.
The assertion giving the values of a_i's is easy to see. For the second assertion when $d = p$, a prime, consider $n - \sum_{i \geq 0} a_i$ and feed the values of a_i from the first assertion. We obtain

$$n = \sum_i a_i = (p-1)([n/p] + [n/p^2] + \cdots + [n/p^r])$$

which gives the assertion using de Polignac's formula.

1 Arithmetic Functions

Some examples of arithmetic functions are $\mu(n), \phi(n), d(n), \sigma(n), \sigma_k(n), \omega(n), \Omega(n)$.
An arithmetic function f is *multiplicative* if it is not identically zero (equivalently $f(1) \neq 0$) and $f(mn) = f(m)f(n)$ for all $(m, n) = 1$.
The functions $\mu(n), \phi(n), d(n), \sigma(n), \sigma_k(n)$ are multiplicative. The proof is by induction on the number of prime divisors and depends on the observation that divisors of mp^r for $(m, p) = 1$ with p prime, are of the form dp^s with $d|m$ and $0 \leq s \leq r$.
We leave it for you to write out; we will give a general proof that includes all these cases.
The values of a multiplicative function are determined by the values at prime powers. For prime powers, we have:

$$\phi(p^r) = p^r(1 - 1/p);$$

$$d(p^r) = r + 1;$$

$$\sigma_k(p^r) = \frac{p^{k(r+1)} - 1}{p^k - 1};$$

The proof of multiplicativity A function f is completely multiplicative if it is not the zero function and $f(mn) = f(m)f(n)$ for all m, n.
The k-th power function $n \mapsto n^k$ is completely multiplicative.
The *Liouville function*

$$\lambda(\prod_{i=1}^{r} p_i^{a_i}) = (-1)^{a_1 + \cdots + a_r}$$

is completely multiplicative.

1.1 Dirichlet Convolution

Given arithmetic functions f, g we have a "convolution product" defined by

$$(f * g)(n) = \sum_{ab=n} f(a)g(b) = \sum_{d|n} f(d)g(n/d).$$

Combining with the natural addition $f + g$, we have a commutative ring A with unity. The multiplicative identity is the function $I(n) = \delta_{1,n}$; that is $f * I = f$ for all f.

We show now that every arithmetic function f with $f(1) \neq 0$ has a Dirichlet inverse. In fact, clearly we may define the inverse f^{-1} recursively by

$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{d|n, d<n} f^{-1}(d) f(n/d).$$

Rephrasing in terms of Dirichlet series

We shall study later series of the form $\sum_{n\geq 1} \frac{f(n)}{n^s}$ in a complex variable and f is an arithmetic function. The convolution $f * g$ of arithmetic functions corresponds to the product of the corresponding series; that is,

$$F(s) := \sum_n \frac{f(n)}{n^s}, G(s) := \sum_n \frac{g(n)}{n^s}$$

give

$$F(s)G(s) := \sum_n \frac{(f*g)(n)}{n^s}.$$

The inclusion-exclusion principle.
By this title, we mean here the identity $\sum_{d|n} \mu(d) = I(n)$.
If $n = 1$, it is clear. Let $n > 1$ and write $n = \prod_{i=1}^r p_i^{a_i}$ where p_i's are distinct primes. The divisors of n are of the form $\prod_{j\in J} p_j^{b_j}$ where $J \subset \{1, 2, \cdots, r\}$ and $b_j \leq a_j$ for each j. Since μ vanishes on non-(square-free) numbers, the sum

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{i=1}^r \mu(p_i) + \sum_{i\neq j} \mu(p_i p_j) + \cdots + \mu(p_1 p_2 \cdots p_r)$$

$$= \binom{r}{0} - \binom{r}{1} + \binom{r}{2} - \cdots + \binom{r}{r}(-1)^r = (1-1)^r = 0 = I(n).$$

Later, we will see the above from a general result.

1.2 A few problems/properties involving $[x]$

1. The sequence $[n+\sqrt{n}+1/2]$ takes exactly all the non-squares as values.
Proof.
Put $a_n = [n+\sqrt{n}+\frac{1}{2}]$. Then a_n increases and $a_{n^2} = n^2+n$. Hence, consider the integers in the range

$$a_{n^2} + 1 \leq x < a_{(n+1)^2};$$

that is, in $n^2 + n + 1 \leq x \leq (n+1)^2 + (n+1) - 1 = n^2 + 3n + 1$.
There are $2n+1$ natural numbers in this range and this includes the $2n$ values $a_{n^2+1}, \cdots, a_{(n+1)^2-1} = a_{n^2+2n}$. This range contains exactly one perfect square; viz. $(n+1)^2$. Thus, to show that the set if values of the sequence is precisely the set of perfect squares, it suffices to show that a value not taken by the sequence $\{a_n\}$ is a square.
Now, if m is a natural number missed by the sequence, then $a_n < m < a_{n+1}$.
The first inequality $a_n < m$ implies $n + \sqrt{n} + \frac{1}{2} < m$.
The second inequality $m < a_{n+1}$ gives

$$m \leq a_{n+1} - 1 = [n + \sqrt{n+1} + \frac{1}{2}] \leq n + \sqrt{n+1} + \frac{1}{2}.$$

Thus,

$$n + \sqrt{n} + \frac{1}{2} < m \leq n + \sqrt{n+1} + \frac{1}{2}.$$

So,

$$\sqrt{n} < m - n - \frac{1}{2} \leq \sqrt{n+1}$$

which gives

$$n < (m-n)^2 + \frac{1}{4} - m + n \leq n + 1.$$

Hence.

$$-\frac{1}{4} < (m-n)^2 - m \leq \frac{3}{4}$$

which forces $(m-n)^2 = m$.

2. (Beatty's theorem.)
Let α, β be fixed positive real numbers, and consider the integers of the form $[\alpha n]$ and $\beta n]$ as n varies over positive integers. Then, this is exactly the set of all positive intgers, each occurring precisely once, if and only if, $\frac{1}{\alpha} + \frac{1}{\beta} = 1$ and α, β are irrational.
Samuel Beatty was the only doctoral student of Fields.

Beatty sequences are also sometimes called Rayleigh's sequences because one of his theorems states that when a constraint is introduced to a vibrating system, the new frequencies of vibration interleave the old frequencies.
The Beatty sequences when α is the golden ratio gives a strategy for Wythoff's game that we mentioned earlier.

Proof.

Assume first that α, β are irrational, positive, real numbers satisfying $1/\alpha + 1/\beta = 1$. Therefore, $(\alpha - 1)(\beta - 1) = 1$.
We will show that each positive integer occurs exactly once among the union

$$\{[\alpha n] : n \in \mathbb{N}\} \cup \{[\beta n] : n \in \mathbb{N}\}.$$

We do this by giving explicitly an ordering of this union which will make it clear. Consider all fractions of the form u/α and v/β as u, v run through the positive integers. Firstly, we observe that they are all distinct; indeed, if $u/\alpha = v/\beta$, then $u/v = \alpha/\beta = \alpha - 1$ which is irrational, which leads to a contradiction.
Now, let us find the number of fractions smaller than a particular v/β. The fractions of the form $u/\alpha < v/\beta$ are clearly $[v\alpha/\beta]$ in number. Thus, as it is the v-th among fractions of the form a/β, the position of v/β among all the fractions considered is

$$[v\alpha/\beta] + v = [v(\alpha - 1)] + v = [v\alpha].$$

Similarly, the position of u/α is $[u\beta]$. Therefore, every positive integer has a unique position given explicitly as above.
Conversely, suppose α, β are positive real numbers such that every positive integer occurs precisely once among the union

$$\{[\alpha n] : n \in \mathbb{N}\} \cup \{[\beta n] : n \in \mathbb{N}\}.$$

We claim $1/\alpha + 1/\beta = 1$ and that they are irrational. In fact, the first assertion would imply the second because if α is rational, then so is $\beta = \alpha/(\alpha - 1)$, and $[n\alpha]$ and $[n\beta]$ cannot cover all positive integers.
To show $1/\alpha + 1/\beta = 1$, the most natural proof is to look at densities of sequences.
A sequence $\{a_n\}$ of positive integers is said to possesses a *natural density* δ if $\frac{\#(\{a_n\} \leq N)}{N} \to \delta$ as $N \to \infty$.
For any positive real α, the number

$$N(\alpha) := \#\{[n\alpha] \leq N\}$$

is easily seen to satisfy

$$\left[\frac{N+1}{\alpha}\right] - 1 \leq N(\alpha) < \left[\frac{N+1}{\alpha}\right]$$

where equality can occur only when α is rational. Note that the above inequalities show that the sequence $[n\alpha]$ has density $1/\alpha$. Thus, as they disjointly cover all positive integers, we have $1/\alpha + 1/\beta = 1$.
Further, α, β must be irrational.
Remark. A beautiful interpretation of Beatty's theorem is given in the American Math Monthly paper by Ginosar and Yona in Volume 119, October 2012.

3. (This is problem 37 after section 4.1 in NZM but was originally a problem in USAMO 1981): *For any real x and positive integer n, prove that* $\sum_{k=1}^{n}[kx]/k \leq [nx]$.
Firstly, it is clear that the subtlety is in the RHS being $[nx]$ because $LHS \leq \sum_{k=1}^{n} kx/k = nx$.
As the LHS is not an integer, the problem is more difficult.
The proof goes as follows. We apply induction on n and as the proof is clear for $n = 1$, we fix $n > 1$ and assume the result for each $r < n$.
Let x_n denote the maximum among the rational numbers $[kx]/k$; then, $x_n = [n_0x]/n_0$ where n_0 is the smallest such among $1, 2, \cdots, n$.
Now $kx_n \geq [kx]$ which means $[kx_n] \geq [kx]$ for all $k \leq n$.
On the other hand, $x = n_0x/n_0 \geq [n_0x]/n_0 = x_n$ for all $k \leq n$. Thus, $kx \geq kx_n$ which gives the other inequality $[kx] \geq [kx_n]$ for each $k \leq n$. Therefore, we have

$$[kx] = [kx_n] \ \forall \ k \leq n \cdots\cdots\cdots (\spadesuit).$$

If $n_0|n$, we are already done because in that case nx_n is an integer as n_0x_n is, and then

$$[nx] = [nx_n] = nx_n \geq \sum_{k=1}^{n}[kx]/k.$$

Assume $n \equiv r \bmod n_0$ with $0 < r < n_0$, and we will use the induction hypothesis for r.
We claim that x_n is the smallest number satisfying $(\spadesuit)$. Let $y < x_n$. Then $n_0y < n_0x_n = [n_0x]$ which gives $[n_0y] < [n_0x]$ which means y does not satisfy $(\spadesuit)$ for $k = n_0$.
Now, recall we have $n \equiv r \bmod n_0$ where $0 < r < n_0$. Now, $n - r$ being a

multiple of n_0, $(n-r)x_n$ is an integer, Hence

$$[nx] = [nx_n] = [rx_n + (n-r)x_n] = [rx_n] + (n-r)x_n.$$

In order to use the induction hypothesis that $[rx_n] \geq \sum_{k=1}^{r}[kx]/k$, we rewrite the last expression on the right in terms of the difference $[rx_n] - \sum_{k=1}^{r}[kx]/k$. We have

$$[nx_n] = [rx_n] + (n-r)x_n = [rx_n] - \sum_{k=1}^{r}[kx_n]/k + \sum_{k=r+1}^{n}\{kx_n\}/k + \sum_{k=1}^{n}[kx_n]/k \geq \sum_{k=1}^{n}[kx_n]/k.$$

Therefore,

$$[nx] = [nx_n] \geq \sum_{k=1}^{n}[kx_n]/k = \sum_{k=1}^{n}[kx]/k.$$

4. Exercise 36 after section 4.1 of NZM.
Prove

$$LCM(1, 2, \cdots, n+1) = (n+1)LCM(\binom{n}{1}, \binom{n}{2}, \cdots, \binom{n}{n}).$$

Solution.
Firstly, $(n+1)\binom{n}{r} = (r+1)\binom{n+1}{r+1}$ which means $r+1$ divides RHS above. Hence, in the asserted equality, the LHS divides the RHS.
For the converse, we present a beautiful proof by Mohan Nair.
In the next property below, we give another proof which was also used to prove a prime number estimate.
We will show that $(r+1)\binom{n+1}{r+1}$ divides the LHS $LCM(1, 2, \cdots, n+1)$.
Fix n. For each $r \leq n$, consider the definite integral

$$I(r) = \int_0^1 x^r(1-x)^{n-r}dx.$$

Using the binomial expansion for $(1-x)^{n-r}$, we will obtain

$$I(r) = \sum_{j=0}^{n-r}(-1)^j\binom{n-r}{j}\frac{1}{r+j+1}.$$

Therefore, LCM $(1, 2, \cdots, n+1)I(r) \in \mathbb{Z}$. On the other hand, using the so-called Beta-Gamma identity (look up the formula and accept it without

proof for now!) and using the fact that $\Gamma(d) = (d-1)!$ for a positive integer, we have

$$I(r) = \beta(r+1, n-r+1) = \frac{\Gamma(r+1)\Gamma(n-r+1)}{\Gamma(n+2)} = \frac{(r!)(n-r)!}{(n+1)!} = \frac{1}{(r+1)\binom{n+1}{r+1}}.$$

Hence, since $LCM(1, 2, \cdots, n+1)I(r) \in \mathbb{Z}$, we have that this LCM is a multiple of $(r+1)\binom{n+1}{r+1}$ for each $r \leq n$.

5. Here is a property involving the ceiling function $\lceil x \rceil$:
(a) $\lceil n/2 \rceil \binom{n}{\lceil n/2 \rceil} > 2^n$ if $n > 6$.
(b) Further, $\operatorname{lcm}(1, 2, \ldots, n) = \operatorname{lcm}\left(2\binom{n}{2}, 3\binom{n}{3}, \ldots, n\binom{n}{n}\right)$.
Therefore, $\operatorname{lcm}(1, 2, \ldots, n) > 2^n$ for $n > 6$.
Note that on changing n to $n+1$ in (b), this is just the previous exercise.

Proof.
The property (a) follows easily by induction on $n > 6$. For $n = 7$, we have $4\binom{7}{4} = 140 > 2^7$. We assert

$$(n+1)\binom{2n+2}{n+1} = 2(n+1)\binom{2n+1}{n+1},$$

$$(n+2)\binom{2n+3}{n+2} > 4(n+1)\binom{2n+1}{n+1}.$$

These are easy to see and imply that the assumption $(n+1)\binom{2n+1}{n+1} > 2^{2n+1}$ leads to the conclusion $\lceil n/2 \rceil \binom{n}{\lceil n/2 \rceil} > 2^n$ for $n > 6$.

For (b), we make use of the little observation below that interprets the power of a prime dividing the lcm being considered:
For a natural number n, if p^a is the highest power of a prime p dividing $\operatorname{lcm}(1, 2, \ldots, n)$, then $p^a \leq n < p^{a+1}$. In other words, $a+1$ is the number of digits of n when written in base p.
Indeed, consider any prime p dividing $\operatorname{lcm}(1, 2, \ldots, n)$; then $p \leq n$. If a is the largest integer so that $p^a \leq n$, then p^a evidently divides $\operatorname{lcm}(1, 2, \ldots, p^a, \ldots, n)$. As the power of p dividing $\operatorname{lcm}(1, 2, \ldots, n)$ is the maximum of the powers of p dividing the numbers $1, 2, \ldots, n$, it follows that p^{a+1} does not divide $\operatorname{lcm}(1, 2, \ldots, n)$ as $n < p^{a+1}$. Thus, $p^a \leq n < p^{a+1}$ clearly implies that the number of digits of n written in base p is $a+1$.

Finally, to prove (b), firstly, it is evident that left-hand side is at most equal to the right-hand side because each of $2, 3, \ldots, n$ divides the numbers on the right-hand side whose least common multiple is being considered.
To prove the other inequality, we will prove that the power of p dividing $r\binom{n}{r}$ for any $0 < r < n$ is less than the number $a+1$ of digits of n in base p (and, hence, is at most a). This will imply our assertion. We use the Kummer formula asserting that the power of p dividing a binomial coefficient $\binom{n}{r}$ $(0 < r < n)$ is the number of carry-overs while adding r and $n-r$ written in base p.

Write

$$r = * * \cdots * 0 \cdots 0$$

in base p where there are precisely $u \geq 0$ zeros at the end.

Next, observe that if $n = r + (n-r)$ in base p and n has $a+1$ digits in base p, then at most a of those digits incorporate a carry, since the top digit does not incorporate a carry. As r ends in precisely u zeros in base p, those u places do not propagate carries, and the first digit of n that includes a carry from earlier places is place $u+1$ or later. Thus, the number of carries is at most $a-u$. So, the power of p in $r\binom{n}{r}$ is at most $u + (a-u) = a$, and the proof is complete.

2 Arithmetic Functions, Möbius inversion.

Lemma. If f, g are multiplicative, then so is $f * g$. Conversely, if f, g are arithmetic functions such that $f*g$ and one of f, g are multiplicative, then so is the other. In particular, the Dirichlet inverse of a multiplicative function is also multiplicative. That is, the set of multiplicative functions forms a subgroup of the group A^* of units.
Proof.
The proof is very simple. Assume f, g are multiplicative and consider $h = f * g$. Let $(m, n) = 1$. Then

$$h(mn) = \sum_{d|mn} f(d)g(mn/d).$$

Each divisor d of mn is uniquely expressible as $d = ab$, with a unique $a|m$ and a unique $b|n$ because $(m, n) = 1$. Hence,

$$h(mn) = \sum_{a|m,b|n} f(ab)g(mn/ab) = (\sum_{a|m} f(a)g(m/a))(\sum_{b|n} f(b)g(n/b)) = h(m)h(n).$$

We used the fact that $(m/a, n/b) = 1$ and that f, g are multiplicative.

Now, we consider f, g such that g and $f * g$ are multiplicative (note that $*$ is commutative and the assumption is without loss of generality).
We show $f(mn) = f(m)f(n)$ for co-prime m, n by induction on mn.
If $mn = 1$, then $m = n = 1$ and we have

$$1 = h(1)) = f(1)g(1) = f(1)$$

which gives $f(mn) = f(1) = f(1)^2 = f(m)f(n)$.
Let $mn > 1$ and assume that $f(ab) = f(a)f(b)$ for all co-prime a, b such that $ab < mn$. Now

$$h(mn) = \sum_{a|m,b|n} f(ab)g(mn/ab) = \sum_{a|m,b|n,ab<mn} f(ab)g(mn/ab) + f(mn)g(1)$$

$$= \sum_{a|m,b|n,ab<mn} f(a)f(b)g(mn/ab) + f(mn).$$

We have used the fact that $f(ab) = f(a)f(b)$ when $ab < mn$.
Clearly, by the multiplicativity of g, the last sum equals

$$(\sum_{a|m} f(a)g(m/a))(\sum_{b|n} f(b)g(n/b)) - f(m)f(n) + f(mn).$$

That is,

$$h(mn) = h(m)h(n) - f(m)f(n) + f(mn).$$

As h is multiplicative, this forces $f(mn) = f(m)f(n)$.

Finally, the fact that the Dirichlet inverse of a multiplicative function f is multiplicative follows from the previous assertion because $f * f^{-1} = I$ is a multiplicative function where the identity $I(n) = \delta_{1,n}$.
The proof is complete.

Corollary. *An arithmetic function f is multiplicative if, and only if, $g(n) := \sum_{d|n} f(d)$ is.*

Proof.
We note that $g = f * \mathbf{1}$ where $\mathbf{1}$ is the constant function 1 which is evidently multiplicative.

Remark.
For a completely multiplicative function f (that is, $f(mn) = f(m)f(n)$ for all m, n), the Dirichlet inverse is simply $f^{-1}(n) = \mu(n)f(n)$. This is checked by using the above inclusion-exclusion principle.

Möbius inversion formula

For an arbitrary arithmetic function f (not necessarily multiplicative), we have $g(n) = \sum_{d|n} f(d)$ if, and only if, $f(n) = \sum_{d|n} g(d)\mu(n/d)$.
Proof.
The assertion is equivalent to showing $g = f * \mathbf{1}$ if, and only if, $f = g * \mu$. Clearly, the inclusion-exclusion principle above asserts that $\mu * \mathbf{1} = I$; that is, the Dirichlet inverse of μ is $\mathbf{1}$.

2.1 Some examples of Möbius inversion formulae

1
The Möbius inversion formula also has a multiplicative version which can be proved using the same ideas but can also be deduced by considering logarithms when the function is positive. The assertion is:
If $f(n) > 0$ for all n, we have

$$g(n) = \prod_{d|n} f(d) \Leftrightarrow f(n) = \prod_{d|n} g(d)^{\mu(n/d)}.$$

As a consequence, we have the cyclotomic polynomial expressed as

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

More generally, let $a(n)$ be a real-valued arithmetic function with $a(1) \neq 0$, and let $b(n)$ be its Dirichlet inverse. Then,

$$g(n) = \prod_{d|n} f(d)^{a(n/d)} \Leftrightarrow f(n) = \prod_{d|n} g(d)^{b(n/d)}.$$

2. *$\phi(n) = \sum_{d|n} d\mu(n/d) = n \sum_{d|n} \mu(d)/d$; that is, $\phi = Id * \mu$ where Id is the identity function. Cautionary note: The identity function is NOT the*

identity in the ring A.
Indeed, counting the n-th roots of unity according to their orders, we have $n = \sum_{d|n} \phi(d)$; that is $Id = \phi * \mathbf{1}$. Since $\mu^{-1} = \mathbf{1}$, we have the identity.
By the way, here is another way to see $\sum_{d|n} \phi(d) = n$. Count the n fractions $1/n, 2/n, \cdots, n/n$ in their reduced forms. Clearly, those with a particular denominator $d|n$ are exactly $\phi(d)$ in number!

3. *The Liouville function λ satisfies $\sum_{d|n} \lambda(d) = sq(n)$, where $sq(n) = 1$ if n is a perfect square, and 0, otherwise. The Dirichlet inverse of λ is $|\mu|$.*
As the LHS $\sum_{d|n} \lambda(d)$ is multiplicative, we may calculate it by computing on prime powers. We obtain the value at p^a to be 0 or 1 according as to whether a is odd or even. This clearly gives the value at any n to be 0 if n is not a perfect square and the value 1 when n is a square.
Finally, by complete multiplicativity of λ, we have $\lambda^{-1}(n) = \mu(n)\lambda(n)$. But, evidently

$$\mu(n)(\lambda(n) - \mu(n)) = 0.$$

Therefore $\mu(n)\lambda(n) = \mu(n)^2 = |\mu(n)|$.

4. *The Dirichlet inverse of σ_r is given by $\sigma_r^{-1}(n) = \sum_{d|n} d^r \mu(d)\mu(n/d)$.*
In fact, $\sigma_r = N_r * \mathbf{1}$ where N_r is the r-th power map. Therefore,

$$\sigma_r^{-1} = \mathbf{1}^{-1} * N_r^{-1} = \mu * (\mu N_r)$$

because N_r is completely multiplicative.

5. *Define the von Mangoldt function Λ by $\Lambda(n) = \log\ p$ if n is a power of p, and equals 0 otherwise. Then, $\Lambda(n) = \sum_{d|n} \mu(d) \log(n/d)$; that is, $\Lambda = \log * \mu$.*
(Recall that we had used this identity while discussing a geometric problem that involved cyclotomic polynomials.)
Indeed, if $n = \prod_{i=1}^{r} p_i^{a_i}$, taking logarithms gives us

$$\log\ n = \sum_{i=1}^{r} a_i \log\ p_i.$$

Now, $\sum_{d|n} \Lambda(d) = \sum_{p_i^k|n} \log\ p_i = \sum_{i=1}^{r} a_i \log\ p_i$ because the powers of p_i dividing n are $1, 2, \cdots, a_i$ which are a_i in number.
Thus,

$$\log\ n = \sum_{d|n} \Lambda(d)$$

which means $\log = \Lambda * \mathbf{1}$. Therefore, $\Lambda = \log * \mu$.

A beautiful geometric application.
Let $n > 1$ and let $P_1, \cdots, P_n$ be points on a circle of radius 1 dividing the circumference into n equal parts. Then, the product of lengths $\prod_{(l,n)=1, l<n} |\overline{P_1 P_{l+1}}| = p$ or 1 accordingly as to whether $n = p^k$ for a prime p or n is not a power of a prime.
To answer this, we may assume that the origin is the center and that points are $P_{d+1} = e^{2id\pi/n}$ for $d = 0, 1, \cdots, n-1$. Note that the product of lengths of all the chords $P_1 P_i$ is simply $\prod_{d=1}^{n-1} |1 - e^{2id\pi/n}|$. Since the polynomial $1 + X + \cdots + X^{n-1}$ has as roots all the n-th roots of 1 excepting 1 itself, we have

$$\prod_{d=1}^{n-1} (1 - e^{2id\pi/n}) = n$$

by evaluating at $X = 1$. Notice that we have the equality $\prod_{d=1}^{n-1}(1 - e^{2id\pi/n}) = n$ as complex numbers; that is, even without considering absolute values.
Now, let us consider our problem. Here, the product under consideration is

$$\prod_{(d,n)=1} |1 - e^{2id\pi/n}|.$$

Writing $P(n) = \prod_{l=1}^{n-1}(1-\zeta^l)$ and $Q(n) = \prod_{(d,n)=1}(1-\zeta^d)$, where $\zeta = e^{2i\pi/n}$, we can see that

$$P(n) = \prod_{r|n} Q(r).$$

By Möbius inversion, $Q(n) = \prod_{d|n} P(d)^{\mu(n/d)} = \prod_{d|n} d^{\mu(n/d)}$ by the simpler first assertion observed at the beginning of the pr of the proposition. The function

$$\log Q(n) = \sum_{d|n} \mu(n/d) \log(d)$$

can be identified with the so-called von Mangoldt function $\Lambda(n)$ which is defined to have the value $\log(p)$ if n is a power of p and 0 otherwise. Using this identification, exponentiation gives also the value asserted in the proposition; viz., $Q(n) = p$ or 1 according as to whether n is a power of a prime p or not.
To see why $\Lambda(n) = \sum_{d|n} \mu(n/d) \log(d)$, we write $n = \prod_{p|n} p^{v_p(n)}$ and note that

$$\log(n) = \sum_{p|n} v_p(n) \log(p)$$

But, the right hand side is clearly $\sum_{d|n} \Lambda(d)$. Hence, Möbius inversion yields

$$\Lambda(n) = \sum_{d|n} \log(d)\mu(n/d).$$

2.2 Exercises on arithmetic functions

• *Prove* $\frac{n}{\phi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\phi(d)}$.
Solution.
As the function $\mu^2(n)/\phi(n)$ is multiplicative, (and so is the LHS), we need to check the identity on prime powers only. But,
$\text{RHS}(p^r) = \sum_{k=0}^{1} \mu^2(p^k)/\phi(p^k) = 1 + 1/(p-1) = \frac{1}{1-1/p} = \text{LHS}(p^r)$.

• *Prove that* $\sum_{d^k|n} \mu(d) = 0$ *if* $m^k|n$ *for some* $m > 1$, *and* $= 1$ *otherwise. In particular, for* $k = 2$, *we get the RHS to be* $\mu^2(n)$.
Solution.
If $m^k|n$ implies $m = 1$, then the value is clearly 1. Suppose now that $m^k|n$ for some $m > 1$ and we write

$$n = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} = PQ$$

say, where $0 < a_i < k$; $b_i \geq k$ and $P = \prod_i p_i^{a_i}, Q = \prod_j q_j^{b_j}$. Then, the sum is

$$\sum_{d^k|PQ} \mu(d) = \sum_{d_1^k|P, d_2^k|Q} \mu(d_1 d_2)$$

since $(P, Q) = 1$. Therefore, only terms with $d_1 = 1$ survive and the sum equals

$$\sum_{d_2^k|Q} \mu(d_2) = \sum_{kc_j \leq b_j} \mu(\prod_j q_j^{c_j})$$

$$= \sum_{c_j=0,1} \prod_j \mu(q_j^{c_j}) = \prod_j (\mu(1) + \mu(q_j)) = 0.$$

• *Prove that* $\sum_{d|n} \mu(d) \log^m(d) = 0$ *if* $m \geq 1$ *and* n *has more than* m *distinct prime factors.*
Solution.
We apply induction on $m \geq 1$. If $m = 1$ and n has at least two prime factors, then $\sum_{d|n} \mu(d) \log(d) = \Lambda(n) = 0$. Assume $m > 1$ and that the result holds for $m - 1$. Let $n = kp^r$ with $(p, k) = 1$, $\omega(n) > m$; that is, $\omega(k) > m - 1$. Then,

$$\sum_{d|n} \mu(d) \log^m(d) = \sum_{d_1|k, d_2|p^r} \mu(d_1)\mu(d_2) \log^m(d_1 d_2)$$

in which only the terms corresponding to $d_2 = 1, p$ survive. Therefore, the sum is

$$\sum_{d_1|k} \mu(d_1)\Big(\mu(1)\log^m(d_1)+\mu(p)\log^m(d_1p)\Big) = \sum_{d_1|k} \mu(d_1)\Big(\log(d_1)^m-(\log(d_1)+\log(p))^m\Big)$$

$$= -\sum_{d_1|k} \mu(d_1)\left(\binom{m}{1}\log(d_1)^{m-1}\log(p)+\cdots+\binom{m}{m}\log(p)^m\right) = 0$$

where the last equality is by induction hypothesis since $\omega(k) > m-1$.

• *Prove that* $\prod_{t|n} t = n^{d(n)/2}$.
Solution. Combine each $d|n$ with n/d.

• *Prove* $\sum_{r|n} d(r)^3 = \Big(\sum_{r|n} d(r)\Big)^2$.
Solution.
As the functions appearing in the sums are multiplicative, it suffices to check the identity for prime powers. Then

$$\sum_{r|p^k} d(r)^3 = \sum_{l=0}^{k} d(p^l)^3 = \sum_{l=0}^{k} (l+1)^3$$

$$= 1^3+2^3+\cdots+(k+1)^3 = (1+2+\cdots+(k+1))^2 = \left(\sum_{r|p^k} d(r)\right)^2.$$

• *Let* $\phi_k(n)$ *denote the sum of the* k*-th powers of the numbers* $\leq n$ *and coprime to* n*. Note* $\phi_0 = \phi$*, Prove*

$$\sum_{d|n} \frac{\phi_k(d)}{d^k} = \frac{1^k+2^k+\cdots+n^k}{n^k}.$$

Solution.
Express each $\frac{r^k}{n^k}$ as a reduced fraction. If $(r,n) = d$, then writing $r = dR, n = dN$, we have $\frac{r^k}{n^k} = \frac{R^k}{N^k}$ in reduced form. As $R \leq N, (R,N) = 1$, there are exactly $\phi(N)$ fractions in reduced form with denominator N^k. As N runs through the divisors of n, we get the asserted equality.

• *Prove that an even number is perfect if, and only if, it is of the form* $2^{p-1}(2^p-1)$ *where* 2^p-1 *is prime.*

Solution.
It is easy to see that if $2^p - 1$ is prime, then p is prime and

$$\sigma(2^{p-1})\sigma(2^p - 1) = (2^p - 1)2^p$$

which shows that $2^{p-1}(2^p - 1)$ is perfect. This was known to Euclid's school already! For the converse proved by Euler, assume $n = 2^a m$ is perfect where $a > 0$ and m is odd. Obviously $m > 1$ as 2^a cannot be perfect. We are given

$$2^{a+1}m = \sigma(2^a m) = (2^{a+1} - 1)\sigma(m).$$

Thus, since 2^{a+1} and $2^{a+1} - 1$ are co-prime, we have $2^{a+1} - 1$ divides m. Write

$$m = (2^{a+1} - 1)M.$$

Then, $2^{a+1}M = \sigma(m) = \sigma((2^{a+1} - 1)M)$.
If $M > 1$, then m would have distinct divisors $1, M, 2^{a+1} - 1, m$ and perhaps other divisors. So, we would have

$$\sigma(m) \geq 1 + M + (2^{a+1} - 1) + (2^{a+1} - 1)M = 2^{a+1}M + 2^{a+1} > 2^{a+1}M = \sigma(m),$$

a contradiction. Hence $M = 1$; so, $m = 2^{a+1} - 1$ and $\sigma(m) = 2^{a+1} = m + 1$ which means m must be prime.

• *Prove that* $f(n) = [\sqrt{n}] - [\sqrt{n-1}]$ *is a multiplicative function which is not completely multiplicative.*
Solution.
If n is not a perfect square, say $r < \sqrt{n} < r + 1$, then $r \leq \sqrt{n-1}$, which shows $f(n) = 0$. If n is a perfect square, clearly $f(n) = 1$. Obviously, f is multiplicative.
As $f(p^2) = 1 \neq 0 = f(p)^2$ for any prime p, it is not completely multiplicative.

• **A result due to Erdős:**
If g is totally multiplicative, $f(1) \neq 0$ and monotonically increasing, then there exists a constant $c \geq 0$ such that $g(n) = n^c$ for all n.
To see this, it is convenient to call an arithmetic function f totally additive if $f(mn) = f(m) + f(n)$ for all m, n. If we show that any totally additive, monotonically increasing function f must admit a constant $c \geq 0$ satisfying $f(n) = c\log(n)$ for all n, then $g(n) = e^{f(n)}$ would satisfy the assertion. So, we prove the additive version below.
Let $p \neq q$ be primes. We can find infinite sequences $\{a_n\}$ and $\{b_n\}$ of positive integers such that

$$p^{a_n} < q^{b_n} < p^{a_n+1}.$$

So, $a_n \log(p) < b_n \log(q) < (a_n + 1)\log(p)\ \forall\ n \geq 1$; and hence

$$\frac{a_n}{b_n} < \frac{\log(q)}{\log(p)} < \frac{a_n}{b_n} + \frac{1}{b_n}.$$

Therefore, the sequence a_n/b_n converges to $\log(q)/\log(p)$. As f is totally additive, and monotonically increasing, the inequalities $p^{a_n} < q^{b_n} < p^{a_n+1}$ imply

$$a_n f(p) < b_n f(q) < (a_n + 1)f(p)\ \forall\ n \geq 1.$$

Thus, the sequence a_n/b_n converges also to $f(q)/f(p)$. Hence, we have obtained

$$\frac{f(p)}{f(q)} = \frac{\log(p)}{\log(q)}$$

for any two distinct primes $p \neq q$. Fixing one of them, say $q = 2$, we get $f(p) = c\log(p)$ where $c = f(2)/\log(2)$. As p is arbitrary, and c is independent of it, the total additivity shows $f(n) = c\log(n)$ for all n.

3 Binary Recurrences

The Fibonacci sequence is ubiquitous in the scientific world, right from the petals of a sunflower to strategies for two-person games. This sequence is defined by the recursion:

$$F_{n+2} = F_{n+1} + F_n \quad \forall \quad n \geq 0$$

and the initial values $F_0 = 0, F_1 = 1$. The first few terms are

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \cdots$$

Given a similar recurrence $u_{n+2} = au_{n+1} + bu_{n+1}$ for some fixed constants a, b and initial values u_1, u_2, can the sequence $\{u_n\}$ be determined in closed form? Indeed, not only can this recursion be solved, the method can treat any linear recursion

$$u_{n+k} = a_k u_{n+k-1} + \cdots + a_1 u_n$$

with constants a_i's and k initial values $u_0, \cdots, u_{k-1}$. The method is simple, and depends on the roots of the so-called 'characteristic polynomial' of the recurrence:

$$p(x) = x^k - a_k x^{k-1} - \cdots - a_2 x - a_1.$$

Note that if u is a root of $p(x)$, then $u_n := u^n$ is a sequence that solves the recurrence because

$$u^k = a_k u^{k-1} + \cdots + a_1$$

implies

$$u^{n+k} = a_k u^{n+k-1} + \cdots + a_1 u^n.$$

We will just discuss recurrences of order 2; that is, $k = 2$. The characteristic polynomial of the recurrence $u_{n+2} = au_{n+1} + bu_n$ is

$$p(x) = x^2 - ax - b.$$

We may assume $b \neq 0$; otherwise, clearly the recurrence is simply a geometric progression. The polynomial $p(x)$ has roots u, v say.

Case I. Suppose first $u \neq v$.

Then, we claim that every sequence $\{u_n\}$ solving the recurrence can be written as $u_n = su^n + tv^n$ for all n, where the constants s, t are determined by the two equations

$$u_0 = s + t;$$

$$u_1 = su + tv.$$

This is the matrix equation $\begin{pmatrix} 1 & 1 \\ u & v \end{pmatrix} \begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} u_0 \\ u_1 \end{pmatrix}$.

Evidently, there is a unique solution s, t because the matrix $\begin{pmatrix} 1 & 1 \\ u & v \end{pmatrix}$ is invertible. For these s, t, we have $u_n = su^n + tv^n$ simply by induction on n (with the cases $n = 0, 1$ validated by the way s, t are obtained). Indeed, assuming this valid for n and $n + 1$, we have

$$u_{n+2} = au_{n+1} + bu_n = a(su^{n+1} + tv^{n+1}) + b(su^n + tv^n)$$

$$= su^n(au + b) + tv^n(av + b) = su^{n+2} + tv^{n+2}.$$

Case II. If $u = v$.
In this case $p(x) = (x - u)^2$; that is, $a = 2u$ and $b = -u^2$.
Note that the sequence $\{nu^n\}$ is a solution of the recurrence because

$$a(n + 1)u^{n+1} + bnu^n = 2u(n + 1)u^{n+1} - u^2nu^n = (n + 2)u^{n+2}.$$

Once again, given any sequence $\{u_n\}$ solving the recurrence, we may determine s, t uniquely satisfying $u_n = su^n + tnu^n$ for all n. Indeed, s, t are determined by the equations for $n = 0, 1$; that is,

$$u_0 = s; u_1 = su + tu.$$

That is, $s = u_0, t = u_1 - uu_0$.