Maths 4 Number Theory 2012

0. Reference books

There are no books I know of that contain all the material of the course. however, there are many texts on Number Theory in the library. Here are a small selection of them.

- Course in p-adic analysis by Alain M. Robert, Springer GTM 2000.
  Library: QA241 Rob.
- A friendly introduction to number theory by J. H. Silverman, Prentice Hall, 2001.
  QA241 Sil
- Introduction to the theory of numbers by G.H. Hardy and E.M. Wright.
  QA241 Har.
- Introduction to the theory of numbers by Ivan Niven and Herbert S. Zuckerman.
  QA241 Niv.
- Introduction to number theory by Lo-keng Hua Springer-Verlag, 1982.
  QA241 Hua

1. The integer part (= floor) function

Definition 1. For $x \in \mathbb{R}$, $\lfloor x \rfloor$ denotes the *floor*, or *integer part* of x. It is defined as the largest integer $\leq x$.

So we have $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. The graph of $\lfloor x \rfloor$ is a 'staircase' function, constant on $[n, n+1)$ and a jump of 1 at n, for each $n \in \mathbb{Z}$.

Note that for $x > 0$, $\lfloor x \rfloor$ is the number of positive integers $\leq x$. Alternative notation is $[x]$. It looks like a trivial function, but it satisfies some surprising identities (as well as some not-so-surprising ones!)

Proposition 1.1. *For $x \in \mathbb{R}$ and $n \in \mathbb{N}$ we have*

(i) $\lfloor k + x \rfloor = k + \lfloor x \rfloor$ *for* $k \in \mathbb{Z}$, $x \in \mathbb{R}$.
(ii) $\left\lfloor \frac{\ell}{n} + \delta \right\rfloor = \left\lfloor \frac{\ell}{n} \right\rfloor$ *for* $\ell \in \mathbb{N}$ *and* $0 \leq \delta < \frac{1}{n}$.
(iii)

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor nx \rfloor .$$

Proof. (i) and (ii) are easy. For (iii), note that if it is true for x then, using (i), it is true for $x + k$, $k \in \mathbb{Z}$ (k is added to both sides), so we can assume that $0 \leq x < 1$.

Now write $x = \frac{\ell}{n} + \delta$ $(0 \le \delta < \frac{1}{n})$ for ℓ/n the largest rational with denominator n that is $\le x$. Then $0 \le \ell < n$ and for $j = 0, 1, \ldots, n-1$

$$\begin{aligned}\left\lfloor x + \frac{j}{n} \right\rfloor &= \left\lfloor \frac{\ell}{n} + \delta + \frac{j}{n} \right\rfloor \\ &= \left\lfloor \frac{\ell + j}{n} \right\rfloor \qquad \text{(using (ii))} \\ &= \begin{cases} 1 \text{ if } j \ge n - \ell; \\ 0 \text{ otherwise.} \end{cases}\end{aligned}$$

So the LHS of (iii) sums to ℓ. But its RHS is $\lfloor nx \rfloor = \lfloor \ell + n\delta \rfloor = \ell$, as $n\delta < 1$. Hence RHS=LHS. □

Proposition 1.2. *Let $r_1, \ldots, r_k \in \mathbb{R}$. Then*

$$\sum_{i=1}^{k} \lfloor r_i \rfloor \le \left\lfloor \sum_{i=1}^{k} r_i \right\rfloor \le \sum_{i=1}^{k} \lfloor r_i \rfloor + k - 1.$$

Proof. If it's true for all $r_i \in [0, 1)$ then it's true for all r_i (just add an integer N to some r_i, which adds N to $\lfloor r_i \rfloor$ and N to $\left\lfloor \sum_{i=1}^{k} r_i \right\rfloor$. Do this for each i.). So we can assume that all $r_i \in [0, 1)$, giving all $\lfloor r_i \rfloor = 0$ and $0 \le \sum_{i=1}^{k} r_i < k$ and hence $0 \le \left\lfloor \sum_{i=1}^{k} r_i \right\rfloor \le k - 1$. □

These two inequalities are both best possible of their type, since the left one has equality when all the r_i are integers, and the right one has equality when all the r_i are in $[\frac{k-1}{k}, 1)$.

Corollary 1.3. *Let $n = n_1 + \cdots + n_k$, where the n_i are in $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Then the multinomial coefficient*

$$\binom{n}{n_1, \ldots, n_k} = \frac{n!}{n_1! n_2! \ldots n_k!} = B$$

say, is an integer.

Proof. From Problem Sheet 1, Q8(a) we know that for each prime p the power of p that divides $n!$ is $\sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor$, a finite sum. So the power of p dividing B is

$$\begin{aligned}\sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor - \sum_{i=1}^{k} \sum_{j=1}^{\infty} \left\lfloor \frac{n_i}{p^j} \right\rfloor &= \sum_{j=1}^{\infty} \left(\left\lfloor \frac{n}{p^j} \right\rfloor - \sum_{i=1}^{k} \left\lfloor \frac{n_i}{p^j} \right\rfloor \right) \\ &\ge 0,\end{aligned}$$

by the above Proposition, on putting $r_i = n_i/p^j$. Thus B is divisible by a nonnegative power of p for every prime p, so must be an integer. □

Another way to prove that this number is an integer is to show that it is the coefficient of $x_1^{n_1} \ldots x_k^{n_k}$ in the expansion of $(x_1 + \cdots + x_k)^n$.

Say that $p, q \in \mathbb{N}$ are *coprime* (or *relatively prime*) if $\gcd(p, q) = 1$.

Proposition 1.4. *Let p and q be two coprime odd positive integers. Then*

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

We shall see later that this result will be used in the proof of the Law of Quadratic Reciprocity.

Proof. Consider the rectangle with corners $(0,0)$, $(p/2,0)$, $(0,q/2)$ and $(p/2,q/2)$. (Suggest you draw it, along with its diagonal from $(0,0)$ to $(p/2,q/2)$, and the horizontal axis the k-axis, the vertical axis the ℓ-axis. The diagonal is then the line with equation $\ell = kq/p$.) We count the number of integer lattice points (k,ℓ) strictly inside this rectangle in two different ways. First we note that these points form a rectangle with corners

$$(1,1), (\frac{p-1}{2},1), (1,\frac{q-1}{2}), (\frac{p-1}{2},\frac{q-1}{2}),$$

so that there are $\frac{p-1}{2} \cdot \frac{q-1}{2}$ of them in all.

On the other hand, we count separately those below and above the diagonal. Below the diagonal we have, for $k = 1, \ldots \frac{p-1}{2}$ that $\left\lfloor \frac{kq}{p} \right\rfloor$ is the number of points (k,ℓ) with $1 \le \ell \le \frac{kq}{p}$, i.e., below the diagonal, in the kth column. So the total is $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$.

To count the number of lattice points above the diagonal, we flip the diagram over, reversing the rôles of p and q, and of k and ℓ. Then we get that the number of points above the diagonal is $\sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor$. It remains to check that there are no lattice points actually *on* the diagonal. For if the integer lattice point (k,ℓ) were on the diagonal $\ell = kq/p$ we would have $\ell p = kq$ so that, as p and q are coprime, $p \mid k$. But $k < p$, so this is impossible. □

As an exercise, can you state and prove the variant of this result in the case that p and q, while still odd, need not be coprime?

One should also be aware of the following variants of $\lfloor x \rfloor$:

- The *ceiling of* x, $\lceil x \rceil$, is the least integer $\ge x$. Note that $\lceil x \rceil = -\lfloor -x \rfloor$.
- The *nearest integer to* x (no standard notation) can be defined either as $\lfloor x + \frac{1}{2} \rfloor$, where then the nearest integer to $\frac{1}{2}$ is 1, or as $\lceil x - \frac{1}{2} \rceil$, where then the nearest integer to $\frac{1}{2}$ is 0.