Math 221 Winter 2023, Lecture 11: Elementary number theory

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wd`

3. Elementary number theory

3.6. Prime numbers (cont'd)

3.6.6. p-valuations (cont'd)

Recall the last definition from Lecture 10:

Definition 3.6.8. Let p be a prime.

(a) Let n be a nonzero integer. Then, $v_p(n)$ shall denote the largest $m \in \mathbb{N}$ such that $p^m \mid n$. (Thus, $v_p(n)$ is the number of times that you can divide n by p without getting a non-integer.)

This number $v_p(n)$ will be called the **p-valuation** (or the **p-adic valuation**) of n.

(b) In order to have $v_p(n)$ defined for all integers n (as opposed to just for nonzero n), we also define $v_p(0)$ to be ∞ (because 0 can be divided by p an arbitrary number of times without any changes). This symbol ∞ is not an actual number, but we shall pretend that it behaves like a number at least in some regards. In particular, we will eventually add or compare it to other numbers. In doing so, we shall follow the rules that

$$\begin{aligned}
k + \infty = \infty + k = \infty & \qquad \text{for all } k \in \mathbb{Z}; \\
\infty + \infty = \infty; & \\
k < \infty \text{ and } \infty > k & \qquad \text{for all } k \in \mathbb{Z}; \\
\max\{\infty, k\} = \max\{k, \infty\} = \infty & \qquad \text{for all } k \in \mathbb{Z}; \\
\min\{\infty, k\} = \min\{k, \infty\} = k & \qquad \text{for all } k \in \mathbb{Z}.
\end{aligned}$$

Thus, ∞ acts like a "mythical number that is larger than any actual number". We can keep up this charade as long as we only add and compare, but never subtract ∞ from anything (since $1 + \infty = \infty$ would turn into $1 = 0$ if you subtracted ∞).

Here are some examples:

- We have

$$v_3(99) = 2 \qquad \left(\text{since } 3^2 \mid 99 \text{ but } 3^3 \nmid 99\right);$$
$$v_3(98) = 0 \qquad \left(\text{since } 3^0 \mid 98 \text{ but } 3^1 \nmid 98\right);$$
$$v_3(96) = 1 \qquad \left(\text{since } 3^1 \mid 96 \text{ but } 3^2 \nmid 96\right);$$
$$v_3(0) = \infty.$$

We can restate the definition of $v_p(n)$ in yet another way: If p is a prime and n is a positive integer, then $v_p(n)$ is the number of zeroes at the end of the base-p representation of the number n. For example, the base-2 representation of the number 344 is 101011000, which has three zeroes at its end (the other zeroes don't count!), so that $v_2(344) = 3$.

Note that Definition 3.6.8 can be generalized to any positive integer $p > 1$ (prime or not). But most of the useful properties of p-valuations hold only when p is prime.

Let us now discuss some basic properties of p-valuations. We begin with a lemma that is almost trivial, but quite helpful:

Lemma 3.6.9. Let p be a prime. Let $i \in \mathbb{N}$ and $n \in \mathbb{Z}$. Then, $p^i \mid n$ if and only if $v_p(n) \geq i$.

Proof. If $n = 0$, then this is clear (because in this case, we have both $p^i \mid 0 = n$ and $v_p(n) = v_p(0) = \infty \geq i$).

It remains to deal with the case $n \neq 0$. In this case, $v_p(n)$ is defined as the largest $m \in \mathbb{N}$ such that $p^m \mid n$. Thus, in this case, we have $p^i \mid p^{v_p(n)} \mid n$ whenever $i \leq v_p(n)$, whereas $p^i \nmid n$ whenever $i > v_p(n)$. In other words, we have $p^i \mid n$ if and only if $v_p(n) \geq i$. Thus, Lemma 3.6.9 is proved in this case as well. □

Recall some standard notations: For any two numbers x and y, we let $\min\{x, y\}$ denote the smaller of these two numbers, and we let $\max\{x, y\}$ denote the larger of these two numbers. More generally, if S is a set of numbers, then $\min S$ means the smallest element of S (if it exists), and $\max S$ means the largest element of S (if it exists).

Now, we can state a bunch of rather important properties of p-valuations:

Theorem 3.6.10 (basic properties of p-valuations)**.** Let p be a prime. Then:
(a) We have $v_p(ab) = v_p(a) + v_p(b)$ for any $a, b \in \mathbb{Z}$.
(b) We have $v_p(a+b) \geq \min\left\{v_p(a),\ v_p(b)\right\}$ for any $a, b \in \mathbb{Z}$.
(c) We have $v_p(1) = 0$.
(d) We have $v_p(p) = 1$.
(e) We have $v_p(q) = 0$ for any prime $q \neq p$.

Proof. **(a)** Let $a, b \in \mathbb{Z}$. We must prove that $v_p(ab) = v_p(a) + v_p(b)$.

If $a = 0$, then this is saying that $\infty = \infty + v_p(b)$, which follows from our rules for ∞ (specifically, from the rules saying that $\infty + k = \infty$ for all $k \in \mathbb{Z}$ and that $\infty + \infty = \infty$). Likewise, we can prove our claim if $b = 0$.

It thus remains to handle the case when neither a nor b is 0. So let us consider this case. Since a and b are nonzero, the numbers $v_p(a)$ and $v_p(b)$ are nonnegative integers. Let us call give them names: We set

$$n = v_p(a) \qquad \text{and} \qquad m = v_p(b).$$

Thus, $p^n \mid a$ and $p^m \mid b$. In other words, there are integers x and y such that $a = p^n x$ and $b = p^m y$. Consider these x and y.

If we had $p \mid x$, then we would readily obtain $p^{n+1} \mid a$ (because $p \mid x$ entails that $x = pz$ for some integer z, and thus this integer z must satisfy $a = p^n \underbrace{x}_{=pz} = p^n pz = p^{n+1} z$) and therefore $v_p(a) \geq n+1$ (by Lemma 3.6.9, applied to $n+1$ and a instead of i and n), which would contradict $v_p(a) = n < n+1$. Thus, we cannot have $p \mid x$. For similar reasons, we cannot have $p \mid y$.

However, multiplying $a = p^n x$ with $b = p^m y$, we obtain $ab = p^n x \cdot p^m y = p^{n+m} xy$, and thus $p^{n+m} \mid ab$. Therefore, $v_p(ab) \geq n+m$ (by Lemma 3.6.9, applied to ab and $n+m$ instead of n and i).

Now, we shall show that this inequality is an equality. To do so, we must show that $p^{n+m+1} \nmid ab$.

To prove this, we assume the contrary. Thus, $p^{n+m+1} \mid ab = p^{n+m} xy$. Dividing both sides of this divisibility by p^{n+m}, we obtain $p \mid xy$.

However, the prime divisor separation theorem (Theorem 3.6.5 in Lecture 10) says that if the prime number p divides a product of two integers, then it must divide one of these two integers. Therefore, from $p \mid xy$, we obtain either $p \mid x$ or $p \mid y$ (since x and y are integers). But this contradicts the fact that we cannot have $p \mid x$ and we cannot have $p \mid y$. This contradiction shows that our assumption must have been wrong. Thus, we have shown that $p^{n+m+1} \nmid ab$.

So we know that $p^{n+m} \mid ab$ but $p^{n+m+1} \nmid ab$. In other words, the largest $i \in \mathbb{N}$ that satisfies $p^i \mid ab$ is $n+m$. In other words, $v_p(ab) = n+m$ (by the definition of $v_p(ab)$). Since $n = v_p(a)$ and $m = v_p(b)$, we can rewrite this as $v_p(ab) = v_p(a) + v_p(b)$. This proves Theorem 3.6.10 **(a)**.

(b) Let $a, b \in \mathbb{Z}$. We must prove that $v_p(a+b) \geq \min\left\{v_p(a),\ v_p(b)\right\}$.

If $\min\left\{v_p(a),\ v_p(b)\right\} = \infty$, then this inequality boils down to $\infty \geq \infty$ (because $\min\left\{v_p(a),\ v_p(b)\right\} = \infty$ yields $v_p(a) = \infty$ and $v_p(b) = \infty$, so that $a = 0$ and $b = 0$, and thus $a + b = 0$ as well, which in turn leads to $v_p(a+b) = \infty$), which is true.

Thus, it remains to handle the case when $\min\left\{v_p(a),\ v_p(b)\right\} \neq \infty$. Thus, $\min\left\{v_p(a),\ v_p(b)\right\} \in \mathbb{N}$. Set $k = \min\left\{v_p(a),\ v_p(b)\right\}$. Then, $k \leq v_p(a)$ and $k \leq v_p(b)$. From $k \leq v_p(a)$, we obtain $v_p(a) \geq k$ and thus $p^k \mid a$ (by Lemma 3.6.9, applied to $n = a$ and $i = k$). Similarly, $p^k \mid b$. Thus, a and b are multiples

of p^k. Hence, their sum $a+b$ is also a multiple of p^k. In other words, $p^k \mid a+b$. Using Lemma 3.6.9, this in turn entails $v_p(a+b) \geq k = \min\left\{v_p(a), v_p(b)\right\}$. Thus, Theorem 3.6.10 **(b)** is proved.

(c) This follows from $p^0 = 1 \mid 1$ and $p^1 = p \nmid 1$.

(d) This follows from $p^1 = p \mid p$ and $p^2 \nmid p$.

(e) Let $q \neq p$ be a prime. Then, the only positive divisors of q are 1 and q (since q is a prime). Hence, p is not a positive divisor of q (since $p \neq 1$ and $p \neq q$). Therefore, p is not a divisor of q (since p is positive). In other words, $p \nmid q$. Now, from $p^0 = 1 \mid q$ and $p^1 = p \nmid q$, we obtain $v_p(q) = 0$. This proves Theorem 3.6.10 **(e)**. □

Corollary 3.6.11. Let p be a prime. Then,

$$v_p(a_1 a_2 \cdots a_k) = v_p(a_1) + v_p(a_2) + \cdots + v_p(a_k)$$

for any k integers $a_1, a_2, \ldots, a_k$.

Proof. Induct on k. The base case uses $v_p(1) = 0$. The induction step relies on Theorem 3.6.10 **(a)**. □

Note that Theorem 3.6.10 **(a)** would fail if p were allowed to be non-prime. For instance, $v_4(2 \cdot 2) = 1$ but $v_4(2) + v_4(2) = 0 + 0 = 0$.

Let us take a closer look at 2-valuations. The sequence

$$\begin{aligned}&(v_2(1),\ v_2(2),\ v_2(3),\ v_2(4),\ v_2(5),\ \ldots)\\ &= (0,\ 1,\ 0,\ 2,\ 0,\ 1,\ 0,\ 3,\ 0,\ 1,\ 0,\ 2,\ 0,\ 1,\ 0,\ 4,\ \ldots)\end{aligned}$$

is called the **ruler sequence**, as it resembles the pattern of markings on a ruler (a small marking at every inch, a slightly larger marking every 2 inches, an even larger marking every 4 inches, and so on). It tends to appear every once in a while in seemingly unexpected places. Case in point:

Proposition 3.6.12. Let $n \in \mathbb{N}$.

In Section 1.1 (in Lecture 1), we proposed a strategy for solving the Tower of Hanoi puzzle with n disks. Let S_n be this strategy.

Let $k \in \{1, 2, \ldots, 2^n - 1\}$. Then, the k-th move of the strategy S_n moves the $(v_2(k)+1)$-th smallest disk.

Thus, in particular, every odd move (i.e., the 1-st, the 3-rd, the 5-th, and so on moves) moves the smallest disk (since $v_2(k) = 0$ when k is odd).

The proof of Proposition 3.6.12 relies on the following lemma about p-valuations:

Lemma 3.6.13. Let p be a prime. Let $m \in \mathbb{N}$. Let k be an integer such that $p^m \nmid k$. Then, $v_p\left(p^m + k\right) = v_p\left(k\right)$.

Proof of Lemma 3.6.13. From $p^m \nmid k$, we obtain $k \neq 0$, so that $v_p\left(k\right) \neq \infty$. In other words, $v_p\left(k\right) \in \mathbb{N}$.

Let $i = v_p\left(k\right)$. Thus, $i \in \mathbb{N}$ (since $v_p\left(k\right) \in \mathbb{N}$), and the definition of $v_p\left(k\right)$ shows that $p^i \mid k$ and $p^{i+1} \nmid k$.

If we had $m \leq i$, then we would have $p^m \mid p^i \mid k$, which would contradict $p^m \nmid k$. Thus, we cannot have $m \leq i$. In other words, we have $i < m$. Thus, $i \leq m-1$ (since i and m are integers), so that $i+1 \leq m$. Therefore, $p^{i+1} \mid p^m$.

From the definition of p-valuations, it follows easily that $v_p\left(p^m\right) = m$ and $v_p\left(-p^m\right) = m$.

The numbers p^m and k are multiples of p^i (since $p^i \mid p^{i+1} \mid p^m$ and $p^i \mid k$). Thus, their sum $p^m + k$ is a multiple of p^i as well. In other words, $p^i \mid p^m + k$.

On the other hand, let us show that $p^{i+1} \nmid p^m + k$. Indeed, assume the contrary. Thus, $p^{i+1} \mid p^m + k$.

Therefore, the numbers $p^m + k$ and $-p^m$ are multiples of p^{i+1} (since $p^{i+1} \mid p^m + k$ and $p^{i+1} \mid p^m \mid p^m \cdot (-1) = -p^m$). Hence, their sum $\left(p^m + k\right) + \left(-p^m\right)$ is a multiple of p^{i+1} as well. In other words, k is a multiple of p^{i+1} (since $\left(p^m + k\right) + \left(-p^m\right) = k$). But this contradicts $p^{i+1} \nmid k$.

This contradiction shows that our assumption was wrong. Hence, $p^{i+1} \nmid p^m + k$ is proved.

Combining $p^i \mid p^m + k$ with $p^{i+1} \nmid p^m + k$, we see that i is the largest $j \in \mathbb{N}$ satisfying $p^j \mid p^m + k$. In other words, $i = v_p\left(p^m + k\right)$. Hence, $v_p\left(p^m + k\right) = i = v_p\left(k\right)$. This proves Lemma 3.6.13. □

Proof of Proposition 3.6.12. We will prove Proposition 3.6.12 by induction on n:

Base case: If $n = 0$, then there exists no $k \in \{1, 2, \ldots, 2^n - 1\}$ (since the set $\{1, 2, \ldots, 2^n - 1\} = \{1, 2, \ldots, 2^0 - 1\} = \{1, 2, \ldots, 0\}$ is empty in this case). Thus, in this case, Proposition 3.6.12 is vacuously true (i.e., true because it makes a claim about non-existing objects).

Induction step: Let n be a positive integer. Assume (as the induction hypothesis) that Proposition 3.6.12 holds for $n-1$ instead of n. We must now prove that Proposition 3.6.12 holds for n as well.

So let $k \in \{1, 2, \ldots, 2^n - 1\}$ be arbitrary. We must prove that the k-th move of the strategy S_n moves the $(v_2\left(k\right) + 1)$-th smallest disk.

Lemma 3.6.13 (applied to 2, $n-1$ and $k - 2^{n-1}$ instead of p, m and k) yields

$$v_2\left(2^{n-1} + k - 2^{n-1}\right) = v_2\left(k - 2^{n-1}\right),$$

so that

$$v_2\left(k - 2^{n-1}\right) = v_2\left(\underbrace{2^{n-1} + k - 2^{n-1}}_{=k}\right) = v_2\left(k\right). \tag{1}$$

Recall that the strategy S_n was defined recursively: It consists of first performing the strategy S_{n-1} (but with pegs 2 and 3 swapped), then moving the largest disk (from peg 1 to peg 3), and then again performing the strategy S_{n-1} (but now with pegs 1 and 2 swapped). Since strategy S_{n-1} requires $2^{n-1} - 1$ moves in total, we thus conclude that

1. the first $2^{n-1}-1$ moves of strategy S_n are identical with the corresponding moves of strategy S_{n-1} (except that pegs 2 and 3 are swapped);
2. the 2^{n-1}-th move of strategy S_n consists in moving the largest disk;
3. the next $2^{n-1}-1$ moves of strategy S_n (that is, the moves numbered $2^{n-1}+1$, $2^{n-1}+2$, $\ldots$, 2^n-1) are identical with the moves of strategy S_{n-1} (except that pegs 1 and 2 are swapped).

Therefore, the k-th move of the strategy S_n

- moves the same disk as the k-th move of S_{n-1} if $k < 2^{n-1}$;
- moves the largest disk if $k = 2^{n-1}$;
- moves the same disk as the $\left(k-2^{n-1}\right)$-th move of S_{n-1} if $k > 2^{n-1}$.

We thus distinguish between the following three cases:
Case 1: We have $k < 2^{n-1}$.
Case 2: We have $k = 2^{n-1}$.
Case 3: We have $k > 2^{n-1}$.

Let us first consider Case 1. In this case, we have $k < 2^{n-1}$. Thus, the k-th move of the strategy S_n moves the same disk as the k-th move of S_{n-1} (according to the first of the three bullet points above). But our induction hypothesis shows that the latter move moves the $(v_2(k)+1)$-th smallest disk (since $k \in \{1,2,\ldots,2^n-1\}$ and $k < 2^{n-1}$ entails $k \in \left\{1,2,\ldots,2^{n-1}-1\right\}$). Thus, the former move also moves the $(v_2(k)+1)$-th smallest disk. So the claim we are trying to prove has been proved in Case 1.

Let us now consider Case 2. In this case, we have $k = 2^{n-1}$. Thus, the k-th move of the strategy S_n moves the largest disk (according to the second of the three bullet points above), i.e., the n-th smallest disk (since there are n disks in total, so the largest disk is the n-th smallest). However, we have $k = 2^{n-1}$ and thus $v_2(k) = v_2\left(2^{n-1}\right) = n-1$, so that $n = v_2(k)+1$. Thus, the k-th move of the strategy S_n moves the $(v_2(k)+1)$-th smallest disk (because we have shown that it moves the n-th smallest disk). So the claim we are trying to prove has been proved in Case 2.

Let us finally consider Case 3. In this case, we have $k > 2^{n-1}$. Thus, the k-th move of the strategy S_n moves the same disk as the $\left(k-2^{n-1}\right)$-th move of S_{n-1} (according to the third of the three bullet points above). But our induction hypothesis (applied to $k-2^{n-1}$ instead of k) yields that the latter move moves the $\left(v_2\left(k-2^{n-1}\right)+1\right)$-th smallest disk (since $k \in \{1,2,\ldots,2^n-1\}$ and $k > 2^{n-1}$ entails $k-2^{n-1} \in \left\{1,2,\ldots,2^{n-1}-1\right\}$ quite easily[1]). Thus, the former move moves the $\left(v_2\left(k-2^{n-1}\right)+1\right)$-th smallest disk as well. In view of (1), we can restate this as follows: The former move moves the $(v_2(k)+1)$-th smallest disk. So the claim we are trying to prove has been proved in Case 3.

Thus, we have proved our claim in all three Cases 1, 2 and 3. In other words, we have shown that the k-th move of the strategy S_n moves the $(v_2(k)+1)$-th smallest disk. Hence, we have proved that Proposition 3.6.12 holds for n. This completes the induction step. Thus, Proposition 3.6.12 is proved. □

[1]Here are the details: From $k \in \{1,2,\ldots,2^n-1\} \subseteq \mathbb{Z}$ and $k > 2^{n-1}$, we see immediately that $k-2^{n-1}$ is a positive integer. Furthermore, from $k \in \{1,2,\ldots,2^n-1\}$, we obtain $k \leq 2^n-1 = 2\cdot 2^{n-1}-1 = 2^{n-1}+2^{n-1}-1$, so that $k-2^{n-1} \leq 2^{n-1}-1$. Since $k-2^{n-1}$ is a positive integer, this results in $k-2^{n-1} \in \left\{1,2,\ldots,2^{n-1}-1\right\}$.

The ruler sequence also has an appearance in data storage:

Remark 3.6.14. A "Tower of Hanoi" backup scheme is a backup scheme where you have several backup drives for your system. Every odd day, you back up to the first drive. Every even day that is not divisible by 4, you back up to the second drive. Every day that is divisible by 4 but not by 8, you back up to the third drive. And so on. Thus, on the k-th day, you back up to the $(v_2(k)+1)$-th drive. This scheme ensures that at every point in time, you have both a fresh backup and several levels of older backups available.

(Of course, I only said "day" for simplicity; you can use any unit of time instead. Of course, the first drive will see the largest traffic and therefore will wear out and need replacement.)

What is the p-valuation of a factorial $n!$? There turns out to be a nice formula for this:[2]

Theorem 3.6.15 (de Polignac's formula)**.** Let p be a prime. Let $n \in \mathbb{N}$. Then,

$$\begin{aligned} v_p(n!) &= \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \\ &= \left(n//p^1\right) + \left(n//p^2\right) + \left(n//p^3\right) + \cdots . \end{aligned}$$

Proof sketch. First, these sums are infinite sums. Why do they make sense?[3]

Because we can discard all the addends that are zero, and then only finitely many nonzero addends remain. For instance, if $p = 2$ and $n = 13$, then

$$\begin{aligned} &\left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \\ &= \left\lfloor \frac{13}{2^1} \right\rfloor + \left\lfloor \frac{13}{2^2} \right\rfloor + \left\lfloor \frac{13}{2^3} \right\rfloor + \cdots \\ &= \lfloor 6.5 \rfloor + \lfloor 3.25 \rfloor + \lfloor 1.625 \rfloor + \lfloor 0.8125 \rfloor + \lfloor 0.40625 \rfloor + \cdots \\ &= 6 + 3 + 1 + \underbrace{0 + 0 + 0 + 0 + 0 + \cdots}_{\text{These are zeroes, thus don't contribute to the sum}} \\ &= 6 + 3 + 1 = 10, \end{aligned}$$

which is a well-defined (finite) value. More generally, for any prime p and any $n \in \mathbb{N}$, the sum $\left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$ has only finitely many nonzero

[2] See Definition 3.3.12 and Definition 3.3.2 (in Lecture 8) for the notations we are using here. The meaning of the infinite sums will be discussed in the proof of the theorem.

[3] It is trivially easy to concoct an infinite sum that does not make sense: for instance, $1 + 1 + 1 + \cdots$, or $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots$. In general, "infinite" operations in mathematics do not usually exist unless their existence has been justified.

addends (because for every $i \geq n$, we have $p^i \geq p^n > n$ and thus $0 \leq \dfrac{n}{p^i} < 1$, so that $\left\lfloor \dfrac{n}{p^i} \right\rfloor = 0$), and thus becomes a finite sum once we discard all its addends that are zero; but a finite sum obviously has a well-defined value.

Moreover, for every positive integer d, you have $\left\lfloor \dfrac{n}{d} \right\rfloor = n//d$ (by Proposition 3.3.13 in Lecture 8). Thus, the two infinite sums

$$\left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \qquad \text{and}$$
$$\left(n//p^1\right) + \left(n//p^2\right) + \left(n//p^3\right) + \cdots$$

are equal.

It remains to prove that these two sums equal $v_p(n!)$. In other words, we must prove that

$$v_p(n!) = \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots. \tag{2}$$

We can prove this by induction on n:

The *base case* ($n = 0$) boils down to $0 = 0 + 0 + 0 + \cdots$, which is true.

For the *induction step*, we proceed from $n-1$ to n. So we fix a positive integer n, and we assume (as our induction hypothesis) that

$$v_p((n-1)!) = \left\lfloor \frac{n-1}{p^1} \right\rfloor + \left\lfloor \frac{n-1}{p^2} \right\rfloor + \left\lfloor \frac{n-1}{p^3} \right\rfloor + \cdots, \tag{3}$$

and we set out to prove that

$$v_p(n!) = \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots. \tag{4}$$

We first compare the left hand sides: Let $k = v_p(n)$. We know that $n! = (n-1)! \cdot n$, and therefore

$$\begin{aligned} v_p(n!) &= v_p((n-1)! \cdot n) \\ &= v_p((n-1)!) + \underbrace{v_p(n)}_{=k} \qquad \text{(by Theorem 3.6.10 \textbf{(a)})} \\ &= v_p((n-1)!) + k. \end{aligned}$$

In other words, the LHS[4] of (4) equals the LHS of (3) plus k.

Now, we shall show that the RHSs of the two equations differ by k as well.

The main trick is to observe the following:

[4]The word "LHS" means "left hand side".
The word "RHS" means "right hand side".

Claim 1: Let d be a positive integer. Then:

(a) If $d \nmid n$, then $\left\lfloor \frac{n}{d} \right\rfloor = \left\lfloor \frac{n-1}{d} \right\rfloor$.

(b) If $d \mid n$, then $\left\lfloor \frac{n}{d} \right\rfloor = \left\lfloor \frac{n-1}{d} \right\rfloor + 1$.

Claim 1 is Corollary 3.3.17 from Lecture 9, so we need not prove it again.

Now, let $k = v_p(n)$. Then, for each $i \in \{1, 2, \ldots, k\}$, we have $p^i \mid p^k \mid n$ (since $k = v_p(n)$) and therefore

$$\left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{n-1}{p^i} \right\rfloor + 1 \qquad \left(\text{by Claim 1 } \textbf{(b)}\right).$$

On the other hand, for each $i \in \{k+1, k+2, k+3, \ldots\}$, we have $p^i \nmid n$ (since $i > k = v_p(n)$) and thus

$$\left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{n-1}{p^i} \right\rfloor \qquad \left(\text{by Claim 1 } \textbf{(a)}\right).$$

These two equalities together yield

$$\begin{aligned}
&\left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \\
&= \left(\left\lfloor \frac{n-1}{p^1} \right\rfloor + 1 \right) + \left(\left\lfloor \frac{n-1}{p^2} \right\rfloor + 1 \right) + \cdots + \left(\left\lfloor \frac{n-1}{p^k} \right\rfloor + 1 \right) \\
&\qquad + \left\lfloor \frac{n-1}{p^{k+1}} \right\rfloor + \left\lfloor \frac{n-1}{p^{k+2}} \right\rfloor + \left\lfloor \frac{n-1}{p^{k+3}} \right\rfloor + \cdots \\
&= \left(\left\lfloor \frac{n-1}{p^1} \right\rfloor + \left\lfloor \frac{n-1}{p^2} \right\rfloor + \left\lfloor \frac{n-1}{p^3} \right\rfloor + \cdots \right) + k.
\end{aligned}$$

In other words, the RHS of (4) equals the RHS of (3) plus k.

But previously, we have shown the same for the LHSs. Thus, the equality (4) is just the equality (3) with each side increased by k. Since (3) holds (by the induction hypothesis), it thus follows that (4) also holds. In other words,

$$v_p(n!) = \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots.$$

But this completes the induction step, and thus Theorem 3.6.15 is proven.

(For another proof of Theorem 3.6.15, see [19s, Exercise 2.17.2 **(c)**] or [21f5, Theorem 5.3.1].) □

Theorem 3.6.15 is known as **de Polignac's formula** or **Legendre's formula**. Various uses of this formula can be found in [21f5].

3.6.7. Prime factorization

We are now ready to prove one of the most important properties of primes: the fact that every positive integer can be uniquely decomposed into a product of some primes. For instance,

$$200 = 2 \cdot 100 = 2 \cdot 2 \cdot 50 = 2 \cdot 2 \cdot 5 \cdot 10 = \underbrace{2 \cdot 2 \cdot 5 \cdot 2 \cdot 5}_{\text{a product of primes}} .$$

The word "uniquely" means here that any two ways of decomposing a given positive integer n into a product of primes are equal up to reordering the factors. For example, we can also decompose 200 as $5 \cdot 2 \cdot 2 \cdot 5 \cdot 2$, but this is the same product with the factors in a different order.

Let us state this fact in full generality. First, we introduce a name for these decompositions:

Definition 3.6.16. Let n be a positive integer. A **prime factorization** of n means a finite list $(p_1, p_2, \ldots, p_k)$ of primes (not necessarily distinct) such that

$$n = p_1 p_2 \cdots p_k.$$

Thus, $(2,2,5,2,5)$ and $(5,2,2,5,2)$ are prime factorizations of 200. Another such is $(2,2,2,5,5)$. There are more (soon we will perhaps see how many), but all of them contain the number 2 thrice and the number 5 twice (and no other numbers), just as we said.

Let us state this as a general claim:

Theorem 3.6.17 (Fundamental Theorem of Arithmetic)**.** Let n be a positive integer. Then:

(a) There exists a prime factorization of n.

(b) This prime factorization is unique up to reordering its entries. In other words, if $(p_1, p_2, \ldots, p_k)$ and $(q_1, q_2, \ldots, q_\ell)$ are two prime factorizations of n, then $(q_1, q_2, \ldots, q_\ell)$ can be obtained from $(p_1, p_2, \ldots, p_k)$ by reordering the entries.

(c) Let $(p_1, p_2, \ldots, p_k)$ be a prime factorization of n. Let p be any prime. Then, the number of times that p appears in the list $(p_1, p_2, \ldots, p_k)$ (in other words, the number of $i \in \{1, 2, \ldots, k\}$ satisfying $p_i = p$) is $v_p(n)$.

Proof. **(a)** This is Theorem 1.9.6 in Lecture 4.

(c) By the definition of a prime factorization, we have $n = p_1 p_2 \cdots p_k$. Thus,

$$\begin{aligned} v_p(n) &= v_p(p_1 p_2 \cdots p_k) \\ &= v_p(p_1) + v_p(p_2) + \cdots + v_p(p_k) \end{aligned} \tag{5}$$

(by Corollary 3.6.11).

The right hand side of this equality is a sum of k addends. Each of these addends has the form $v_p(p_i)$ for some $i \in \{1,2,\ldots,k\}$. Each such addend $v_p(p_i)$ equals 1 if $p_i = p$ (by Theorem 3.6.10 **(d)**) and equals 0 if $p_i \neq p$ (by Theorem 3.6.10 **(e)**).

Thus, our sum $v_p(p_1) + v_p(p_2) + \cdots + v_p(p_k)$ has an addend equal to 1 for each $i \in \{1,2,\ldots,k\}$ that satisfies $p_i = p$, and an addend equal to 0 for each i that doesn't.

Obviously, the addends that are equal to 0 do not affect the sum. Hence, the sum equals the number of addends equal to 1. In other words, the sum equals the number of $i \in \{1,2,\ldots,k\}$ that satisfy $p_i = p$.

In view of (5), we can restate this as follows: $v_p(n)$ equals the number of $i \in \{1,2,\ldots,k\}$ that satisfy $p_i = p$. In other words, $v_p(n)$ equals the number of times that p appears in the list $(p_1, p_2, \ldots, p_k)$. This proves Theorem 3.6.17 **(c)**.

(b) This follows easily from part **(c)**. Namely:

Let $(p_1, p_2, \ldots, p_k)$ and $(q_1, q_2, \ldots, q_\ell)$ be two prime factorizations of n. We must prove that $(q_1, q_2, \ldots, q_\ell)$ can be obtained from $(p_1, p_2, \ldots, p_k)$ by reordering the entries.

Each prime p appears $v_p(n)$ times in the list $(p_1, p_2, \ldots, p_k)$ (by part **(c)**), and appears $v_p(n)$ times in the list $(q_1, q_2, \ldots, q_\ell)$ (similarly). Thus, each prime p appears the same number of times in either list. Since both lists consist of primes, this shows that the two lists contain the same numbers the same number of times. Therefore, $(q_1, q_2, \ldots, q_\ell)$ can be obtained from $(p_1, p_2, \ldots, p_k)$ by reordering the entries. This proves Theorem 3.6.17 **(b)**.

(We have used the intuitively obvious fact that if two lists of numbers contain the same numbers the same number of times, then one can be obtained from the other by reordering. You are free to trust your intuition on this one; for a formal proof, see [19s, Lemma 2.13.20].) □

Theorem 3.6.17 **(a)** shows that every positive integer n has a prime factorization. Finding this prime factorization is a classical hard computational problem. (Quite a few encryption standards rely on its hardness.)

3.7. Least common multiples

In §3.4 (Lecture 9), we have studied greatest common divisors in some detail. Let me now briefly discuss least common multiples: a kind of counterpart to greatest common divisors. The greatest common divisor of two positive integers a and b is usually smaller than both a and b; in contrast, the least common multiple is usually larger than both.

Definition 3.7.1. Let a and b be two integers.

(a) The **common multiples** of a and b are the integers that are divisible by a and simultaneously divisible by b.

(b) The **least common multiple** (aka the **lowest common multiple**, or just the **lcm**) of a and b is defined as follows:

- If a and b are nonzero, then it is the smallest positive common multiple of a and b.
- Otherwise, it is 0.

It is denoted by $\operatorname{lcm}(a,b)$.

Some examples:

- We have $\operatorname{lcm}(3,4) = 12$.
- We have $\operatorname{lcm}(6,4) = 12$.
- We have $\operatorname{lcm}(6,8) = 24$.
- We have $\operatorname{lcm}(2,4) = 4$.
- We have $\operatorname{lcm}(0,5) = 0$.
- We have $\operatorname{lcm}(-2,3) = 6$.

Note that the lcm of two positive integers is a fairly well-known concept: When you bring two fractions (of integers) to their lowest common denominator, this lowest common denominator is actually the lcm of the denominators of the fractions.

Here are some properties of lcms:

Theorem 3.7.2. Let a and b be two integers. Then:
(a) The lcm of a and b exists.
(b) We have $\operatorname{lcm}(a,b) \in \mathbb{N}$.
(c) We have $\operatorname{lcm}(a,b) = \operatorname{lcm}(b,a)$.
(d) We have $a \mid \operatorname{lcm}(a,b)$ and $b \mid \operatorname{lcm}(a,b)$.
(e) We have $\operatorname{lcm}(-a,b) = \operatorname{lcm}(a,b)$ and $\operatorname{lcm}(a,-b) = \operatorname{lcm}(a,b)$.

Proof sketch. Easy consequences of the definitions. (For part **(a)**, observe that two nonzero integers a and b have at least one positive common multiple – namely, $|ab|$.) □

Here is a counterpart to the universal property of the gcd (Theorem 3.4.8 in Lecture 9):

Theorem 3.7.3 (universal property of the lcm)**.** Let $a, b, m \in \mathbb{Z}$. Then, we have the equivalence

$$(a \mid m \text{ and } b \mid m) \iff (\operatorname{lcm}(a,b) \mid m).$$

In other words, the common multiples of two integers a and b are precisely the multiples of $\operatorname{lcm}(a,b)$.

Proof sketch. (See [19s, Theorem 2.11.7] for a detailed proof.)

$\Longleftarrow$: If $\operatorname{lcm}(a,b) \mid m$, then $a \mid m$ (since Theorem 3.7.2 **(d)** yields $a \mid \operatorname{lcm}(a,b) \mid m$) and $b \mid m$ (similarly). Thus, the "$\Longleftarrow$" direction of the desired equivalence is proved.

$\Longrightarrow$: Assume that $a \mid m$ and $b \mid m$. We must show that $\operatorname{lcm}(a,b) \mid m$.

If one of a and b is 0, then this is easy (in fact, let's say that $a = 0$; then, $0 = a \mid m$, thus $m = 0$, and therefore $\operatorname{lcm}(a,b) \mid 0 = m$). Hence, we need only to consider the case when a and b are nonzero.

In this case, set $\ell = \operatorname{lcm}(a,b)$. Recall that ℓ is defined as the smallest positive common multiple of a and b. Hence, ℓ is a positive integer and is a multiple of a and of b. Let q and r be the quotient and the remainder of the division of m by ℓ. Thus,

$$q \in \mathbb{Z} \qquad \text{and} \qquad r \in \{0,1,\ldots,\ell-1\} \qquad \text{and} \qquad m = q\ell + r$$

(by the definition of quotient and remainder). From $r \in \{0,1,\ldots,\ell-1\}$, we obtain $r < \ell$.

From $m = q\ell + r$, we obtain $r = m - q\ell$. Since both m and ℓ are multiples of a, we thus conclude that r is a multiple of a as well. Similarly, r is a multiple of b. Thus, r is a common multiple of a and b. But ℓ is the smallest positive common multiple of a and b. If r was positive, then r would contradict this minimality (because $r < \ell$). Hence, r cannot be positive. Since $r \in \{0,1,\ldots,\ell-1\}$, we conclude that r must be 0. Hence, $m = q\ell + \underbrace{r}_{=0} = q\ell$, so that $\ell \mid m$. In other words, $\operatorname{lcm}(a,b) \mid m$ (since $\ell = \operatorname{lcm}(a,b)$). This proves the "$\Longrightarrow$" direction of the desired equivalence. $\square$

The gcd and the lcm of two integers are connected to each other by the following formula:

Theorem 3.7.4. Let a and b be two integers. Then,

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|.$$

Proof sketch. (See [19s, Theorem 2.11.6] for a detailed proof.)

First, dispose of the case when a or b is 0. In the remaining case, argue that $\dfrac{ab}{\gcd(a,b)}$ is an integer and is a common multiple of a and b. By Theorem 3.7.3, this entails that $\operatorname{lcm}(a,b) \mid \dfrac{ab}{\gcd(a,b)}$, so that $\gcd(a,b) \cdot \operatorname{lcm}(a,b) \mid ab$. On the other hand, argue (again using Theorem 3.7.3) that $\dfrac{ab}{\operatorname{lcm}(a,b)}$ is an integer

and divides $\gcd(a,b)$ (because it divides each of a and b). Thus conclude that $ab \mid \gcd(a,b) \cdot \operatorname{lcm}(a,b)$. Now, recall that two integers x and y that satisfy $x \mid y$ and $y \mid x$ must satisfy $|x| = |y|$. □

Both gcds and lcms have easily computable p-valuations:

Theorem 3.7.5. Let p be a prime. Let a and b be two integers. Then,

$$v_p(\gcd(a,b)) = \min\left\{v_p(a),\ v_p(b)\right\} \qquad \text{and}$$
$$v_p(\operatorname{lcm}(a,b)) = \max\left\{v_p(a),\ v_p(b)\right\}.$$

Proof sketch. This is a particular case of [19s, Proposition 5.2.15]. Anyway, the proof is a nice exercise in using the universal properties of the gcd and the lcm (and the definition of p-valuation), so you should do it yourself. □

Theorem 3.7.5 gives an easy way to compute $\gcd(a,b)$ and $\operatorname{lcm}(a,b)$ if you know prime factorizations of two positive integers a and b. For example, knowing that $18 = 2 \cdot 3^2$ and $12 = 2^2 \cdot 3$, we obtain

$$\gcd(18,\ 12) = 2 \cdot 3 = 6 \qquad \text{and}$$
$$\operatorname{lcm}(18,\ 12) = 2^2 \cdot 3^2 = 36.$$

If you don't know the prime factorizations of a and b, the quickest way to find $\operatorname{lcm}(a,b)$ is by using the Euclidean algorithm to find $\gcd(a,b)$ first, and then solving the equality $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|$ for $\operatorname{lcm}(a,b)$. This gives[5]

$$\operatorname{lcm}(a,b) = \frac{|ab|}{\gcd(a,b)} = \left|\frac{a}{\gcd(a,b)} \cdot b\right|.$$

Gcds and lcms can be defined for multiple numbers (not just for two numbers). Their properties are mostly analogous to the case of two numbers, with some exceptions (i.e., the formula $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|$ does not generalize to $\gcd(a,b,c) \cdot \operatorname{lcm}(a,b,c) = |abc|$, but rather to $\gcd(a,b,c) \cdot \operatorname{lcm}(bc,ca,ab) = |abc|$). See [19s, §2.11] for more details.

3.8. Sylvester's $xa + yb$ theorem (or the Chicken McNugget theorem)

We come to a rather curious (although not overly important) topic in elementary number theory: the $\mathbb{N}$-linear combinations of two positive integers.

For this entire section, we let a and b be two positive integers.

[5] Here we are assuming that a and b are nonzero. If a or b is 0, then $\operatorname{lcm}(a,b)$ is just 0.

Definition 3.8.1. (a) A **$\mathbb{Z}$-linear combination** (short: **$\mathbb{Z}$-LC**) of a and b will mean a number of the form

$$xa + yb \qquad \text{with } x, y \in \mathbb{Z}.$$

In other words, it means a number of cents that you can pay with a-cent coins and b-cent coins if you can get change.

(b) An **$\mathbb{N}$-linear combination** (short: **$\mathbb{N}$-LC**) of a and b will mean a number of the form

$$xa + yb \qquad \text{with } x, y \in \mathbb{N}.$$

In other words, it means a number of cents that you can pay with a-cent coins and b-cent coins without getting change.

Thus, Proposition 1.9.7 (in Lecture 5) is saying that any integer $n \geq 8$ is an $\mathbb{N}$-LC of 3 and 5. Moreover, as we saw just above that proposition, the numbers $0,\ 3,\ 5,\ 6$ are $\mathbb{N}$-LCs of 3 and 5 as well, whereas the numbers $1,\ 2,\ 4,\ 7$ are not. Thus the complete list of all $\mathbb{N}$-LCs of 3 and 5 is

$$0,\ 3,\ 5,\ 6,\ \underbrace{8,\ 9,\ 10,\ \ldots}_{\text{all integers } n \geq 8}.$$

This should prompt us to study $\mathbb{N}$-LCs of a and b in the general case. We shall begin with the $\mathbb{Z}$-LCs, however, since they are much easier to describe.

Note that the $\mathbb{N}$-LCs of a and b are always ≥ 0 (because if $x, y \in \mathbb{N}$, then $\underbrace{x}_{\geq 0}\underbrace{a}_{>0} + \underbrace{y}_{\geq 0}\underbrace{b}_{>0} \geq 0$), whereas the $\mathbb{Z}$-LCs of a and b can have any sign.

Clearly, any $\mathbb{N}$-LC of a and b is a $\mathbb{Z}$-LC of a and b. However, a $\mathbb{Z}$-LC of a and b doesn't have to be an $\mathbb{N}$-LC of a and b, even if it is ≥ 0. For example, 1 is a $\mathbb{Z}$-LC of 3 and 5 (since $1 = 2 \cdot 3 + (-1) \cdot 5$), but not an $\mathbb{N}$-LC of 3 and 5.

We can easily describe the $\mathbb{Z}$-LCs of a and b:

Proposition 3.8.2. The $\mathbb{Z}$-LCs of a and b are exactly the multiples of $\gcd(a, b)$.

Proof. We must prove the following two claims:

Claim 1: Any $\mathbb{Z}$-LC of a and b is a multiple of $\gcd(a, b)$.

Claim 2: Any multiple of $\gcd(a, b)$ is a $\mathbb{Z}$-LC of a and b.

But both claims are easy:

Proof of Claim 1. Let n be a $\mathbb{Z}$-LC of a and b. We must show that n is a multiple of $\gcd(a, b)$.

Indeed, n is a $\mathbb{Z}$-LC of a and b, and thus has the form $n = xa + yb$ for some $x, y \in \mathbb{Z}$. Consider these x, y. We have $\gcd(a, b) \mid a \mid xa$ and $\gcd(a, b) \mid b \mid yb$. In other words, both numbers xa and yb are multiples of $\gcd(a, b)$. Hence, their sum $xa + yb$ is a multiple of $\gcd(a, b)$ as well. In other words, n is a multiple of $\gcd(a, b)$ (since $n = xa + yb$). This proves Claim 1. $\square$

Proof of Claim 2. Let n be a multiple of $\gcd(a,b)$. We must prove that n is a $\mathbb{Z}$-LC of a and b.

Bezout's theorem (Theorem 3.4.5 in Lecture 9) says that there exist two integers x and y such that $\gcd(a,b) = xa + yb$. Consider these x and y. However, n is a multiple of $\gcd(a,b)$; in other words, there exists an integer c such that $n = \gcd(a,b) \cdot c$. Consider this c. Now,

$$n = \underbrace{\gcd(a,b)}_{=xa+yb} \cdot c = (xa+yb) \cdot c = xac + ybc = (cx)\,a + (cy)\,b.$$

This shows that n is a $\mathbb{Z}$-LC of a and b (since cx and cy are integers). This proves Claim 2. □

Combining Claim 1 with Claim 2, we conclude that the $\mathbb{Z}$-LCs of a and b are exactly the multiples of $\gcd(a,b)$. Thus, Proposition 3.8.2 is proved. □

Now we move on to the $\mathbb{N}$-LCs. What are they? Can we describe them any better than by their definition?

Let $g = \gcd(a,b)$. Then, g divides each of a and b, so that the numbers $\dfrac{a}{g}$ and $\dfrac{b}{g}$ are positive integers. We can simplify our problem by replacing a and b with $\dfrac{a}{g}$ and $\dfrac{b}{g}$. Clearly, the $\mathbb{N}$-LCs of a and b are just the $\mathbb{N}$-LCs of $\dfrac{a}{g}$ and $\dfrac{b}{g}$, multiplied by g. As we know (Theorem 3.5.12 in Lecture 10), the two integers $\dfrac{a}{g}$ and $\dfrac{b}{g}$ are coprime. Thus, understanding the $\mathbb{N}$-LCs of the original integers a and b is equivalent to understanding the $\mathbb{N}$-LCs of the coprime integers $\dfrac{a}{g}$ and $\dfrac{b}{g}$.

Hence, it suffices to solve our problem in the case when a and b are coprime. In this case, Proposition 3.8.2 shows that every integer is a $\mathbb{Z}$-LC of a and b (since every integer is a multiple of $1 = \gcd(a,b)$). The $\mathbb{N}$-LCs are more interesting. We have already listed the $\mathbb{N}$-LCs of 3 and 5 above; let us now give a somewhat more complicated example: The $\mathbb{N}$-LCs of 5 and 9 are

$$0,\ 5,\ 9,\ 10,\ 14,\ 15,\ 18,\ 19,\ 20,\ 23,\ 24,\ 25,\ 27,\ 28,\ 29,\ 30,\ \underbrace{32,\ 33,\ 34,\ \ldots}_{\text{all integers } n \geq 32}.$$

Note that every integer $n \geq 32$ is an $\mathbb{N}$-LC of 3 and 5. Among the first 32 nonnegative integers $0, 1, \ldots, 31$, exactly half (that is, 16) are $\mathbb{N}$-LCs of 5 and 9. A similar phenomenon can be seen in our above example with 3 and 5, except that 32 is replaced by 8.

This phenomenon generalizes:

Theorem 3.8.3 (Sylvester's two-coin theorem, or Chicken McNugget theorem)**.** Assume that the two positive integers a and b are coprime. Then:

(a) Every integer $n > ab - a - b$ is an $\mathbb{N}$-LC of a and b.

(b) The number $ab - a - b$ is **not** an $\mathbb{N}$-LC of a and b.

(c) Among the first $(a-1)(b-1)$ nonnegative integers $0, 1, \ldots, ab-a-b$, exactly half are $\mathbb{N}$-LCs of a and b.

(d) Let $n \in \mathbb{Z}$. Then, exactly one of the two numbers n and $ab - a - b - n$ is an $\mathbb{N}$-LC of a and b.

This theorem was discovered by J. J. Sylvester in 1884, as a side-product of his work in invariant theory. Its more recent moniker is due to the McDonald's Chicken McNuggets, which used to be sold in packs of 9 or 20, prompting mathematicians to wonder what numbers of nuggets could be bought.

The theorem stops short of explicitly answering which of the first $(a-1)(b-1)$ nonnegative integers are $\mathbb{N}$-LCs of a and b. There is no "easy formula" for this answer. But Theorem 3.8.3 **(a)** gives you all the information you need to compute all the $\mathbb{N}$-LCs of a and b, since the first $(a-1)(b-1)$ nonnegative integers can be checked one by one.

The particular case of Theorem 3.8.3 **(a)** where $a = p$ and $b = p+1$ was Exercise 4 on homework set #3.

Before we prove Theorem 3.8.3, we show a basic lemma:

Lemma 3.8.4. Assume that the two positive integers a and b are coprime. Let $n \in \mathbb{Z}$. Then, there exist two integers u and v such that $0 \leq u \leq b-1$ and $ua + vb = n$.

Proof of Lemma 3.8.4. Bezout's theorem (Theorem 3.4.5 in Lecture 9) says that there exist two integers x and y such that $\gcd(a,b) = xa + yb$. Consider these x and y. Thus, $xa + yb = \gcd(a,b) = 1$ (since a and b are coprime).

Recall that b is a positive integer. Thus, division with remainder by b is well-defined (see Definition 3.3.2 in Lecture 8 for the terminology).

Let $q = (nx)\,//\,b$ and $r = (nx)\,\%b$. In other words, let q and r be the quotient and the remainder of the division of nx by b. By the definition of quotient and remainder, we thus have

$$q \in \mathbb{Z} \qquad \text{and} \qquad r \in \{0,1,\ldots,b-1\} \qquad \text{and} \qquad nx = qb + r.$$

From $r \in \{0,1,\ldots,b-1\}$, we see that r is an integer satisfying $0 \leq r \leq b-1$.

On the other hand, $nxa + nyb = n\underbrace{(xa+yb)}_{=1} = n$, so that

$$\begin{aligned} n &= \underbrace{nx}_{=qb+r} a + nyb = (qb+r)\,a + nyb \\ &= qba + ra + nyb = ra + \underbrace{qba + nyb}_{=(qa+ny)b} = ra + (qa+ny)\,b. \end{aligned}$$

In other words, $ra + (qa + ny)\, b = n$.

Altogether, we now know that r and $qa + ny$ are two integers satisfying $0 \leq r \leq b-1$ and $ra + (qa + ny)\, b = n$. Thus, there exist two integers u and v such that $0 \leq u \leq b-1$ and $ua + vb = n$ (namely, $u = r$ and $v = qa + ny$). This proves Lemma 3.8.4. □

Proof of Theorem 3.8.3. We shall first prove part **(b)** and then part **(d)**. The other two parts will follow quite easily from these.

(b) Assume the contrary. Thus, $ab - a - b$ is an $\mathbb{N}$-LC of a and b. In other words, there exist integers x and y such that $ab - a - b = xa + yb$. Consider these x and y.

From $ab - a - b = xa + yb$, we obtain $ab = xa + yb + a + b = (x+1)\, a + (y+1)\, b = a\,(x+1) + b\,(y+1)$. Hence,

$$b\,(y+1) = ab - a\,(x+1) = a \cdot \underbrace{(b - (x+1))}_{\text{an integer}}.$$

This shows that $a \mid b\,(y+1)$. Thus, the coprime removal theorem (Theorem 3.5.6 in Lecture 10) yields that $a \mid y+1$ (since a is coprime to b). Therefore, $\dfrac{y+1}{a}$ is an integer (since $a \neq 0$). Since $\underbrace{y}_{\geq 0} + 1 \geq 1 > 0$ and $a > 0$, this integer $\dfrac{y+1}{a}$ is furthermore positive, and thus is ≥ 1. In other words, $y + 1 \geq a$. Hence, $y \geq a - 1$. Now,

$$ab - a - b = \underbrace{x}_{\geq 0} a + \underbrace{y}_{\geq a-1} b \geq 0a + (a-1)\, b = ab - b.$$

Subtracting $ab - a - b$ from both sides of this inequality, we obtain $0 \geq a$, which contradicts the positivity of a. This contradiction shows that our assumption was false. Thus, Theorem 3.8.3 **(b)** is proved.

(d) Let $m = ab - a - b - n$. Hence, $n + m = ab - a - b$. Thus, $n + m$ is not an $\mathbb{N}$-LC of a and b (since Theorem 3.8.3 **(b)** shows that $ab - a - b$ is not an $\mathbb{N}$-LC of a and b).

We shall now prove the following two claims:

Claim 1: At **least** one of the two numbers n and m is an $\mathbb{N}$-LC of a and b.

Claim 2: At **most** one of the two numbers n and m is an $\mathbb{N}$-LC of a and b.

Proof of Claim 1. Lemma 3.8.4 shows that there exist two integers u and v such that $0 \leq u \leq b-1$ and $ua + vb = n$. Consider these u and v. Now,

$$\begin{aligned}(b-1-u)\, a + (-v-1)\, b &= ba - a - ua - vb - b \\ &= \underbrace{ba}_{=ab} - a - b - \underbrace{(ua + vb)}_{=n} \\ &= ab - a - b - n = m \end{aligned} \tag{6}$$

(by the definition of m). We are in one of the following two cases:

Case 1: We have $v \geq 0$.

Case 2: We have $v < 0$.

Let us first consider Case 1. In this case, we have $v \geq 0$. Thus, $v \in \mathbb{N}$. Also, $u \in \mathbb{N}$ (since $0 \leq u$). Recall that $ua + vb = n$, so that $n = \underbrace{u}_{\in \mathbb{N}} a + \underbrace{v}_{\in \mathbb{N}} b$. This shows that n is an $\mathbb{N}$-LC of a and b. Thus, at least one of the two numbers n and m is an $\mathbb{N}$-LC of a and b. So we have proved Claim 1 in Case 1.

Let us next consider Case 2. In this case, we have $v < 0$. Hence, $-v > 0$, so that $-v \geq 1$ (since $-v$ is an integer) and therefore $-v - 1 \geq 0$. Thus, $-v - 1 \in \mathbb{N}$. Moreover, from $u \leq b - 1$, we obtain $b - 1 - u \geq 0$, so that $b - 1 - u \in \mathbb{N}$. However, (6) yields

$$m = \underbrace{(b - 1 - u)}_{\in \mathbb{N}} a + \underbrace{(-v - 1)}_{\in \mathbb{N}} b.$$

This shows that m is an $\mathbb{N}$-LC of a and b. Thus, at least one of the two numbers n and m is an $\mathbb{N}$-LC of a and b. So we have proved Claim 1 in Case 2.

Thus, Claim 1 holds in each of Cases 1 and 2. The proof of Claim 1 is therefore complete. □

Proof of Claim 2. Assume the contrary. Thus, both numbers n and m are $\mathbb{N}$-LCs of a and b. Therefore, we can write n as $n = xa + yb$ for some $x, y \in \mathbb{N}$ (since n is an $\mathbb{N}$-LC of a and b). Furthermore, we can write m as $m = za + wb$ for some $z, w \in \mathbb{N}$ (since m is an $\mathbb{N}$-LC of a and b). Consider these x, y, z, w. Now, adding the equalities $n = xa + yb$ and $m = za + wb$ together, we obtain

$$n + m = (xa + yb) + (za + wb) = \underbrace{(x + z)}_{\in \mathbb{N}} a + \underbrace{(y + w)}_{\in \mathbb{N}} b.$$

This shows that $n + m$ is an $\mathbb{N}$-LC of a and b. This contradicts the fact that $n + m$ is not an $\mathbb{N}$-LC of a and b. This contradiction shows that our assumption was wrong. Hence, Claim 2 is proved. □

Combining Claim 1 with Claim 2, we see that exactly one of the two numbers n and m is an $\mathbb{N}$-LC of a and b. In other words, exactly one of the two numbers n and $ab - a - b - n$ is an $\mathbb{N}$-LC of a and b (since $m = ab - a - b - n$). This proves Theorem 3.8.3 **(d)**.

(a) Let $n > ab - a - b$. Then, the integer $ab - a - b - n$ is negative, and thus cannot be an $\mathbb{N}$-LC of a and b (since any $\mathbb{N}$-LC of a and b is ≥ 0). However, Theorem 3.8.3 **(d)** yields that exactly one of the two numbers n and $ab - a - b - n$ is an $\mathbb{N}$-LC of a and b. Since $ab - a - b - n$ cannot be an $\mathbb{N}$-LC of a and b, we thus conclude that n is an $\mathbb{N}$-LC of a and b. This proves Theorem 3.8.3 **(a)**.

(c) Consider the following table of integers:

0	1	2	$\cdots\cdots\cdots$	$ab - a - b - 1$	$ab - a - b$
$ab - a - b$	$ab - a - b - 1$	$ab - a - b - 2$	$\cdots\cdots\cdots$	1	0

(whose first row is listing the numbers $0, 1, 2, \ldots, ab - a - b$ in increasing order, while the second row is listing the same numbers in decreasing order). This table has $ab - a - b + 1 = (a - 1)(b - 1)$ many columns.

Each column of this table contains the numbers n and $ab-a-b-n$ for some $n \in \{0,1,\ldots,ab-a-b\}$. Thus, each column of this table contains exactly one $\mathbb{N}$-LC of a and b (by Theorem 3.8.3 **(d)**). Hence, in total, exactly $(a-1)(b-1)$ entries of our table are $\mathbb{N}$-LCs of a and b (since our table has $(a-1)(b-1)$ many columns). Since our table contains each element of the set $\{0,1,\ldots,ab-a-b\}$ exactly twice, this entails that exactly $\dfrac{(a-1)(b-1)}{2}$ elements of this set are $\mathbb{N}$-LCs of a and b. In other words, among the elements of the set $\{0,1,\ldots,ab-a-b\}$, exactly half are $\mathbb{N}$-LCs of a and b. But this is precisely the claim of Theorem 3.8.3 **(c)**. Thus, Theorem 3.8.3 **(c)** is proved. □

Theorem 3.8.3 is one of the deepest results we will see in this course, but it is only the beginning of a theory! See the Wikipedia page for "Coin problem" for more general (and trickier) questions, such as describing the $\mathbb{N}$-LCs of three integers a, b, c. See also the slides of Drew Armstrong's talk at FPSAC 2017 for deep connections to algebraic combinatorics (and a visual proof different from ours).

References

[19s] Darij Grinberg, *Introduction to Modern Algebra (UMN Spring 2019 Math 4281 notes)*, 29 June 2019.
`http://www.cip.ifi.lmu.de/~grinberg/t/19s/notes.pdf`

[21f5] Darij Grinberg, *Math 235 Fall 2021, Worksheet 5: p-valuations*, 29 December 2021.
`https://www.cip.ifi.lmu.de/~grinberg/t/21f/lec5.pdf`