Math 221 Winter 2023, Lecture 9: Elementary number theory

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

3. Elementary number theory

3.3. Division with remainder (cont'd)

3.3.5. Congruence in terms of remainders

Here is one more application of division with remainder: a new criterion for congruence. Specifically, two integers a and b are congruent modulo a given positive integer d if and only if they leave the same remainder when divided by d (that is, satisfy $a\%d = b\%d$). In other words:

Proposition 3.3.15. Let d be a positive integer. Let a and b be two integers. Then, $a \equiv b \operatorname{mod} d$ if and only if $a\%d = b\%d$.

Proof. Proposition 3.3.11 **(a)** from Lecture 8 (applied to $n = a$) yields that $a\%d \in \{0, 1, \ldots, d-1\}$ and $a\%d \equiv a \operatorname{mod} d$. Similarly, $b\%d \in \{0, 1, \ldots, d-1\}$ and $b\%d \equiv b \operatorname{mod} d$.

We must prove the logical equivalence $(a \equiv b \operatorname{mod} d) \iff (a\%d = b\%d)$. In other words, we must prove the two implications

$$(a \equiv b \operatorname{mod} d) \implies (a\%d = b\%d)$$

and

$$(a\%d = b\%d) \implies (a \equiv b \operatorname{mod} d).$$

Let us prove these implications separately:

Proof of $(a \equiv b \operatorname{mod} d) \implies (a\%d = b\%d)$*:* Assume that $a \equiv b \operatorname{mod} d$. Thus, $b \equiv a \operatorname{mod} d$ (by symmetry of congruence – i.e., by Proposition 3.2.4 **(b)** from Lecture 7). Combining $b\%d \equiv b \operatorname{mod} d$ with $b \equiv a \operatorname{mod} d$, we obtain $b\%d \equiv a \operatorname{mod} d$ (by transitivity of congruence – i.e., by Proposition 3.2.4 **(c)** from Lecture 7).

Thus, we know that $b\%d \in \{0, 1, \ldots, d-1\}$ and $b\%d \equiv a \operatorname{mod} d$. Hence, Proposition 3.3.11 **(c)** from Lecture 8 (applied to $n = a$ and $c = b\%d$) yields $b\%d = a\%d$. In other words, $a\%d = b\%d$. Thus, we have proved the implication $(a \equiv b \operatorname{mod} d) \implies (a\%d = b\%d)$.

Proof of $(a\%d = b\%d) \implies (a \equiv b \operatorname{mod} d)$*:* Assume that $a\%d = b\%d$. However, we know that $a\%d \equiv a \operatorname{mod} d$, so that $a \equiv a\%d \operatorname{mod} d$ (by symmetry of congruence). In view of $a\%d = b\%d$, we can rewrite this as $a \equiv b\%d \operatorname{mod} d$. Combining this with $b\%d \equiv b \operatorname{mod} d$, we obtain $a \equiv b \operatorname{mod} d$ (by transitivity of congruence – i.e., by Proposition 3.2.4 **(c)** from Lecture 7). Thus, we have proved the implication $(a\%d = b\%d) \implies (a \equiv b \bmod d)$.

Now, both implications are proved, so that Proposition 3.3.15 is proved. □

3.3.6. The birthday lemma

If you have lived for exactly n days, then you are $n//365$ years and $n\%365$ days old (assuming, for simplicity, that every year has exactly 365 days; leapyears would complicate this a lot). On any "normal" day, the latter number (that is, $n\%365$) increases by 1 while the former number (that is, $n//365$) stays unchanged. But on a birthday, the latter number gets reset to 0 while the former number increases by 1. This simple and intuitive observation is not specific to 365, and is worth stating as a proposition:

> **Proposition 3.3.16** (birthday lemma)**.** Let $n \in \mathbb{Z}$, and let d be a positive integer. Then:
>
> **(a)** If $d \mid n$, then
>
> $$n//d = ((n-1)//d) + 1 \qquad \text{and}$$
> $$n\%d = 0 \qquad \text{and} \qquad (n-1)\%d = d-1.$$
>
> **(b)** If $d \nmid n$, then
>
> $$n//d = (n-1)//d \qquad \text{and} \qquad n\%d = ((n-1)\%d) + 1.$$

It should be easy to prove both parts of this lemma, but we give a proof for the sake of completeness.

Proof of Proposition 3.3.16. **(a)** Assume that $d \mid n$. Thus, $n = dq$ for some $q \in \mathbb{Z}$. Consider this q.

Recall Definition 3.3.2 from Lecture 8. We have $q \in \mathbb{Z}$ and $0 \in \{0, 1, \ldots, d-1\}$ and $n = qd + 0$ (since $qd + 0 = qd = dq = n$). In other words, $(q, 0)$ is a quo-rem pair of n and d (by the definition of a quo-rem pair). Hence, Definition 3.3.2 from Lecture 8 shows that $n//d = q$ and $n\%d = 0$.

On the other hand, from $n = dq$, we obtain

$$\begin{aligned} n - 1 &= dq - 1 \\ &= (q-1)\,d + (d-1) \qquad \left(\text{since } (q-1)\,d + (d-1) = qd - d + d - 1 = qd - 1\right). \end{aligned}$$

Thus, we have $q - 1 \in \mathbb{Z}$ and $d - 1 \in \{0, 1, \ldots, d-1\}$ and $n - 1 = (q-1)\,d + (d-1)$. In other words, the pair $(q-1, d-1)$ is a quo-rem pair of $n-1$ and d (by the definition of a quo-rem pair). Hence, Definition 3.3.2 from Lecture 8 shows that $(n-1)//d = q-1$ and $(n-1)\%d = d-1$.

Now, from $(n-1)//d = q-1$, we obtain $((n-1)//d) + 1 = q = n//d$. In other words, $n//d = ((n-1)//d) + 1$. Combining this with $n\%d = 0$ and $(n-1)\%d = d-1$, we see that Proposition 3.3.16 **(a)** has been proved.

(b) Assume that $d \nmid n$. Let $q = n//d$ and $r = n\%d$. Then, by the definition of quotient and remainder, we have

$$q \in \mathbb{Z} \qquad \text{and} \qquad r \in \{0, 1, \ldots, d-1\} \qquad \text{and} \qquad n = qd + r.$$

If we had $r = 0$, then we would have $n = qd + \underbrace{r}_{=0} = qd = dq$, which would entail $d \mid n$; but this would contradict $d \nmid n$. Hence, we cannot have $r = 0$. In other words, r is not 0.

So r is an element of the set $\{0, 1, \ldots, d-1\}$ but is not 0. Therefore, r is one of the remaining elements $1, 2, \ldots, d-1$. Therefore, $r-1$ is one of the elements $0, 1, \ldots, d-2$. Thus, $r - 1 \in \{0, 1, \ldots, d-1\}$.

Also, from $n = qd + r$, we obtain $n - 1 = (qd + r) - 1 = qd + (r-1)$. So we know that $q \in \mathbb{Z}$ and $r - 1 \in \{0, 1, \ldots, d-1\}$ and $n - 1 = qd + (r-1)$. In other words, the pair $(q, r-1)$ is a quo-rem pair of $n-1$ and d (by the definition of a quo-rem pair). Hence, Definition 3.3.2 from Lecture 8 shows that $(n-1)//d = q$ and $(n-1)\%d = r - 1$.

Thus, $(n-1)//d = q = n//d$, so that $n//d = (n-1)//d$. Also, from $(n-1)\%d = r-1$, we obtain $((n-1)\%d) + 1 = r = n\%d$, so that $n\%d = ((n-1)\%d) + 1$. Thus, we have proved Proposition 3.3.16 **(b)**. □

Part of Proposition 3.3.16 can be restated using the floor notation:

Corollary 3.3.17. Let $n \in \mathbb{Z}$, and let d be a positive integer. Then:

(a) If $d \mid n$, then

$$\left\lfloor \frac{n}{d} \right\rfloor = \left\lfloor \frac{n-1}{d} \right\rfloor + 1.$$

(b) If $d \nmid n$, then

$$\left\lfloor \frac{n}{d} \right\rfloor = \left\lfloor \frac{n-1}{d} \right\rfloor.$$

Proof. Proposition 3.3.13 yields $n//d = \left\lfloor \frac{n}{d} \right\rfloor$. The same argument (applied to $n-1$ instead of n) yields $(n-1)//d = \left\lfloor \frac{n-1}{d} \right\rfloor$.

(a) Assume that $d \mid n$. Then, Proposition 3.3.16 **(a)** yields $n//d = ((n-1)//d) + 1$. In view of $n//d = \left\lfloor \frac{n}{d} \right\rfloor$ and $(n-1)//d = \left\lfloor \frac{n-1}{d} \right\rfloor$, we can rewrite this as $\left\lfloor \frac{n}{d} \right\rfloor = \left\lfloor \frac{n-1}{d} \right\rfloor + 1$. This proves Corollary 3.3.17 **(a)**.

(b) Assume that $d \nmid n$. Then, Proposition 3.3.16 **(b)** yields $n//d = (n-1)//d$. In view of $n//d = \left\lfloor \frac{n}{d} \right\rfloor$ and $(n-1)//d = \left\lfloor \frac{n-1}{d} \right\rfloor$, we can rewrite this as $\left\lfloor \frac{n}{d} \right\rfloor = \left\lfloor \frac{n-1}{d} \right\rfloor$. This proves Corollary 3.3.17 **(b)**. □

3.4. Greatest common divisors

3.4.1. Definition

The following definition plays a crucial role in number theory, particularly in the study of prime numbers that will be the topic of next lecture.

> **Definition 3.4.1.** Let a and b be two integers.
>
> **(a)** The **common divisors** of a and b are the integers that divide a and simultaneously divide b.
>
> **(b)** The **greatest common divisor** of a and b is the largest among the common divisors of a and b, unless $a = b = 0$. In the case $a = b = 0$, it is defined to be 0 instead.
>
> We denote the greatest common divisor of a and b as $\gcd(a, b)$, and we refer to it as the **gcd** of a and b.

We will soon see that this greatest common divisor is well-defined (see Remark 3.4.2 below). But first, some examples:

- What is $\gcd(4, 6)$?

  The divisors of 4 are $-4, -2, -1, 1, 2, 4$.

  The divisors of 6 are $-6, -3, -2, -1, 1, 2, 3, 6$.

  Thus, the common divisors of 4 and 6 are $-2, -1, 1, 2$.

  So the greatest common divisor of 4 and 6 is 2. That is, $\gcd(4, 6) = 2$.

- What is $\gcd(0, 5)$?

  The divisors of 0 are all integers (you cannot list them all).

  The divisors of 5 are $-5, -1, 1, 5$.

  Thus, the common divisors of 0 and 5 are just the divisors of 5, which are $-5, -1, 1, 5$.

  So the gcd is 5. That is, $\gcd(0, 5) = 5$.

- What is $\gcd(0, 0)$?

  The common divisors of 0 and 0 are all integers, so there is no greatest one among them, but we have defined $\gcd(0, 0)$ to be 0. (This is the reason why we had to make an exception for the $a = b = 0$ case in Definition 3.4.1 **(b)**.)

Let us now convince ourselves that $\gcd(a, b)$ is well-defined:

Remark 3.4.2. Let $a, b \in \mathbb{Z}$. We want to show that $\gcd(a, b)$ is well-defined in Definition 3.4.1 **(b)**.

If $a = b = 0$, then this is clear, since we defined this gcd to be 0.

Consider the remaining case – i.e., the case when $a \neq 0$ or $b \neq 0$ (or both).

For instance, let us assume that $a \neq 0$. Then, the divisors d of a all satisfy $|d| \leq |a|$ (since Proposition 3.1.4 **(b)** from Lecture 7 shows that they satisfy $\operatorname{abs} d \leq \operatorname{abs} a$, which in our present notations means $|d| \leq |a|$). In other words, all these divisors are integers in the interval $[-|a|, |a|]$. Hence, there are finitely many of them. Therefore, there are finitely many common divisors of a and b (since any common divisor of a and b is a divisor of a). On the other hand, there is at least one common divisor of a and b (namely, 1). Therefore, the set of all common divisors of a and b is nonempty and finite, and thus has a maximum element. In other words, there is a (literally) largest among the common divisors of a and b. This shows that $\gcd(a, b)$ is well-defined when $a \neq 0$.

An analogous argument leads to the same conclusion when $b \neq 0$. Thus, we have shown that $\gcd(a, b)$ is always well-defined.

This argument also gives us a slow and stupid algorithm to compute $\gcd(a, b)$ when $a \neq 0$: We just go through all integers in the interval $[-|a|, |a|]$, and check which of them are common divisors of a and b. But there is a much faster algorithm.

3.4.2. Basic properties

To find this algorithm, we first collect some basic properties of gcds:

Proposition 3.4.3. **(a)** We have $\gcd(a, b) \in \mathbb{N}$ for any $a, b \in \mathbb{Z}$.

(b) We have $\gcd(a, 0) = \gcd(0, a) = |a|$ for any $a \in \mathbb{Z}$.

(c) We have $\gcd(a, b) = \gcd(b, a)$ for any $a, b \in \mathbb{Z}$.

(d) If $a, b, c \in \mathbb{Z}$ satisfy $b \equiv c \mod a$, then $\gcd(a, b) = \gcd(a, c)$.

(e) We have $\gcd(a, b) = \gcd(a,\ ua + b)$ for any $a, b, u \in \mathbb{Z}$.

(f) We have $\gcd(a, b) = \gcd(a,\ b\%a)$ for any positive integer a and any $b \in \mathbb{Z}$.

(g) We have $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$ for any $a, b \in \mathbb{Z}$.

(h) We have $\gcd(-a, b) = \gcd(a, b)$ and $\gcd(a, -b) = \gcd(a, b)$ for any $a, b \in \mathbb{Z}$.

(i) If $a, b \in \mathbb{Z}$ satisfy $a \mid b$, then $\gcd(a, b) = |a|$.

Proof. **(a)** Let $a, b \in \mathbb{Z}$. We must prove that $\gcd(a, b) \in \mathbb{N}$.

If $a = b = 0$, then this follows from $\gcd(0, 0) = 0 \in \mathbb{N}$.

Thus, let us assume that not both of a and b are 0. Then, $\gcd(a, b)$ is literally the greatest common divisor of a and b. If $\gcd(a, b)$ was negative, then $-\gcd(a, b)$ would be an even greater common divisor of a and b (since

$-\gcd(a,b)$ divides whatever $\gcd(a,b)$ divides, but the negativity of $\gcd(a,b)$ implies $-\gcd(a,b) > \gcd(a,b)$), which would contradict the previous sentence. Hence, $\gcd(a,b)$ cannot be negative. Thus, $\gcd(a,b) \in \mathbb{N}$. This proves Proposition 3.4.3 **(a)**.

(b) Let $a \in \mathbb{Z}$. Every integer is a divisor of 0. Thus, the common divisors of a and 0 are just the divisors of a. However, the largest divisor of a is $|a|$ (unless $a = 0$, which case can be easily handled separately)[1]. Hence, the greatest common divisor of a and 0 is $|a|$. In other words, we have $\gcd(a,0) = |a|$. Similarly, we can see that $\gcd(0,a) = |a|$. Thus, Proposition 3.4.3 **(b)** is proved.

(c) Proposition 3.4.3 **(c)** follows from observing that a and b play equal roles in Definition 3.4.1.

(d) Let $a,b,c \in \mathbb{Z}$ satisfy $b \equiv c \bmod a$. We must prove that $\gcd(a,b) = \gcd(a,c)$.

If $a = 0$, then this is clearly true (because in this case, $b \equiv c \bmod a$ becomes $b \equiv c \bmod 0$, which entails $b = c$).

It thus remains to consider the case $a \neq 0$ only. In this case, $\gcd(a,b)$ is literally the greatest common divisor of a and b, whereas $\gcd(a,c)$ is literally the greatest common divisor of a and c. Hence, in order to prove that these two gcds are equal, it will suffice to show that the common divisors of a and b are precisely the common divisors of a and c. To do this, in turn, it suffices to prove the following two claims:

> *Claim 1:* Each common divisor of a and b is a common divisor of a and c.
>
> *Claim 2:* Each common divisor of a and c is a common divisor of a and b.

Before we prove these two claims, let us recall that $b \equiv c \bmod a$; in other words, $c \equiv b \bmod a$ (by the symmetry of congruence). Hence, the numbers b and c play equal roles in our setting. Thus, Claims 1 and 2 are analogous, so that any proof of one of the two will also prove the other (once the roles of b and c are switched).

Proof of Claim 1. Let d be a common divisor of a and b. Thus, $d \mid a$ and $d \mid b$ (by the definition of a common divisor). In other words, we have $a = dx$ and $b = dy$ for some integers x and y. Consider these x and y.

But $b \equiv c \bmod a$. In other words, $a \mid b - c$. Hence, $d \mid a \mid b - c$ (by the transitivity of divisibility). In other words, $b - c = dz$ for some integer z. Consider this z.

[1] This fact is a consequence of Proposition 3.1.4 **(b)** in Lecture 7 (recalling that $|a|$ was called $\operatorname{abs} a$ back in that proposition).

Now, $b - (b - c) = c$, so that

$$c = \underbrace{b}_{=dy} - \underbrace{(b - c)}_{=dz} = dy - dz = d \underbrace{(y - z)}_{\text{an integer}} .$$

Therefore, $d \mid c$. From $d \mid a$ and $d \mid c$, we conclude that d is a common divisor of a and c.

So we have shown that if d is a common divisor of a and b, then d is a common divisor of a and c. In other words, each common divisor of a and b is a common divisor of a and c. This proves Claim 1. □

Proof of Claim 2. As we said, we can obtain a proof of Claim 2 by switching the roles of b and c in the above proof of Claim 1 (because we have $c \equiv b \bmod a$). □

Combining Claim 1 with Claim 2, we see that the common divisors of a and b are precisely the common divisors of a and c. Therefore, the greatest common divisor of a and b equals the greatest common divisor of a and c. In other words, $\gcd(a, b) = \gcd(a, c)$. This proves Proposition 3.4.3 **(d)**.

(e) Proposition 3.4.3 **(e)** follows from Proposition 3.4.3 **(d)** (applied to $c = ua + b$), since $b \equiv ua + b \bmod a$ (because $b - (ua + b) = -ua$ is divisible by a).

(f) Proposition 3.4.3 **(f)** follows from Proposition 3.4.3 **(d)** (applied to $c = b\%a$), since $b \equiv b\%a \bmod a$ (because Proposition 3.3.11 **(a)** from Lecture 8 yields $b\%a \equiv b \bmod a$).

(g) is obvious when $a = b = 0$ (since $0 \mid 0$), and otherwise follows from the definition of $\gcd(a, b)$.

(h) The divisors of a are precisely the divisors of $-a$. The divisors of b are precisely the divisors of $-b$. Thus, the common divisors of a and b remain unchanged if we replace a by $-a$ or replace b by $-b$. Therefore, Proposition 3.4.3 **(h)** follows from the definition of the gcd.

(i) Let $a, b \in \mathbb{Z}$ satisfy $a \mid b$. Then, $b \equiv 0 \bmod a$. Hence, Proposition 3.4.3 **(d)** (applied to $c = 0$) yields $\gcd(a, b) = \gcd(a, 0) = |a|$ (by Proposition 3.4.3 **(b)**). This proves Proposition 3.4.3 **(i)**. □

Corollary 3.4.4 (Euclidean recursion for the gcd)**.** Let $a \in \mathbb{Z}$, and let b be a positive integer. Then,

$$\gcd(a, b) = \gcd(b,\ a\%b) .$$

Proof. Proposition 3.4.3 **(c)** yields

$$\gcd(a, b) = \gcd(b, a) = \gcd(b,\ a\%b)$$

(by Proposition 3.4.3 **(f)**, applied to b and a instead of a and b). This proves Corollary 3.4.4. □

3.4.3. The Euclidean algorithm

By applying Corollary 3.4.4 repeatedly, we can compute gcds rather quickly: For example,

$$\begin{aligned}
\gcd(93,\ 18) &= \gcd\left(18,\ \underbrace{93\%18}_{=3}\right) && \text{(by Corollary 3.4.4)}\\
&= \gcd(18,\ 3)\\
&= \gcd\left(3,\ \underbrace{18\%3}_{=0}\right) && \text{(by Corollary 3.4.4)}\\
&= \gcd(3,\ 0) = |3| && \text{(by Proposition 3.4.3 \textbf{(b)})}\\
&= 3
\end{aligned}$$

and

$$\begin{aligned}
\gcd(1145,\ 739) &= \gcd\left(739,\ \underbrace{1145\%739}_{=406}\right) && \text{(by Corollary 3.4.4)} \\
&= \gcd(739,\ 406) \\
&= \gcd\left(406,\ \underbrace{739\%406}_{=333}\right) && \text{(by Corollary 3.4.4)} \\
&= \gcd(406,\ 333) \\
&= \gcd\left(333,\ \underbrace{406\%333}_{=73}\right) && \text{(by Corollary 3.4.4)} \\
&= \gcd(333,\ 73) \\
&= \gcd(73,\ 333\%73) && \text{(by Corollary 3.4.4)} \\
&= \gcd(73,\ 41) \\
&= \gcd(41,\ 73\%41) && \text{(by Corollary 3.4.4)} \\
&= \gcd(41,\ 32) \\
&= \gcd(32,\ 41\%32) && \text{(by Corollary 3.4.4)} \\
&= \gcd(32,\ 9) \\
&= \gcd(9,\ 32\%9) && \text{(by Corollary 3.4.4)} \\
&= \gcd(9,\ 5) \\
&= \gcd(5,\ 9\%5) && \text{(by Corollary 3.4.4)} \\
&= \gcd(5,\ 4) \\
&= \gcd(4,\ 5\%4) && \text{(by Corollary 3.4.4)} \\
&= \gcd(4,\ 1) \\
&= \gcd(1,\ 4\%1) && \text{(by Corollary 3.4.4)} \\
&= \gcd(1,\ 0) = |1| && \text{(by Proposition 3.4.3 \textbf{(b)})} \\
&= 1.
\end{aligned}$$

These two computations are instances of a general algorithm for computing $\gcd(a, b)$ for any two numbers $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. This algorithm proceeds as follows:

- If $b = 0$, then the gcd is $|a|$.
- If $b > 0$, then we replace a and b by b and $a\%b$ and recurse (i.e., we apply the method again to b and $a\%b$ instead of a and b).

In Python code, this algorithm looks as follows:

```
def gcd(a, b):  # for b nonnegative
    if b == 0:
        return abs(a) # This is the absolute value of a.
    return gcd(b, a%b)
```

This algorithm is called the **Euclidean algorithm**. Let us convince ourselves that it really terminates (rather than getting stuck in an endless loop):

Proposition 3.4.5. Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then, the Euclidean algorithm terminates after at most b steps. (Here, we count each time that the algorithm replaces a and b by b and $a\%b$ as a "step".)

Proof. In each step of the Euclidean algorithm, the second argument b gets replaced by $a\%b$. This has the consequence that b decreases by at least 1 (since the definition of a remainder yields $a\%b \in \{0, 1, \ldots, b-1\}$ and thus $a\%b \leq b-1$). But b remains nonnegative throughout the algorithm. Thus, b cannot decrease (by at least 1) more than b_0 times in succession, where b_0 is the original value of b (as it was fed into the algorithm). Hence, the algorithm cannot have more than b_0 steps. In other words, the algorithm must terminate after at most b_0 steps. This proves Proposition 3.4.5 (since b_0 is precisely the original value of b). □

Proposition 3.4.5 greatly overestimates the actual time that the Euclidean algorithm needs to terminate: In truth, it terminates after at most $\log_2(ab) + 2$ steps (if a and b are positive)[2], which is usually much fewer than b. Some variants of the Euclidean algorithm get to the goal even faster. This speediness is part of the reason why the Euclidean algorithm (and greatest common divisors) is so useful in practical applications of number theory.

The Euclidean algorithm can be easily adapted to arbitrary $b \in \mathbb{Z}$ instead of just $b \in \mathbb{N}$ (by adding a first step in which we replace b by $-b$ if b is negative):

[2] *Hints to the proof.* Recall that each step of the algorithm replaces the numbers a and b by b and $a\%b$. Since $b > a\%b$ (because $a\%b \in \{0, 1, \ldots, b-1\}$ entails $a\%b < b$), this yields that after each step of the algorithm, the "current" numbers a and b satisfy $a > b$.

Now, consider the product ab of the two numbers a and b. We claim that each step of the algorithm, except perhaps the first one, decreases this number by a factor of at least 2. In order to see this, you need to show that $b(a\%b) \leq \frac{ab}{2}$ whenever $a > b$. But this follows from $a\%b \leq \frac{a}{2}$, which in turn follows easily from $a > b$ (why?).

Now you know that the product ab decreases by a factor of at least 2 at each step of the algorithm except for the first one. In other words, its binary logarithm $\log_2(ab)$ decreases by at least 1 at each step of the algorithm except for the first one. At the first step, it also decreases or stays unchanged. From this, it follows easily that the algorithm cannot have more than $\log_2(ab) + 1$ steps until it reaches a situation in which $\log_2(ab) \leq 0$. But in such a situation, we must have $a = b = 1$, and it will only take one more step to reach the end of the algorithm.

```
def gcd(a, b):  # for b arbitrary
    if b < 0:
        return gcd(a, -b) # replace b by -b.
    if b == 0:
        return abs(a) # This is the absolute value of a.
    return gcd(b, a%b)
```

3.4.4. Bezout's theorem and the extended Euclidean algorithm

The Euclidean algorithm can be adapted so that it doesn't only compute $\gcd(a,b)$, but also expresses $\gcd(a,b)$ as an "integer linear combination" of a and b (that is, as a multiple of a plus a multiple of b). This allows us to prove the following theorem:

> **Theorem 3.4.6** (Bezout's theorem for integers)**.** Let a and b be two integers. Then, there exist two integers x and y such that
>
> $$\gcd(a,b) = xa + yb.$$

We will soon prove this theorem. First, we introduce a notation and give a few examples:

> **Definition 3.4.7.** Let a and b be two integers. Then, a **Bezout pair** for (a,b) means a pair (x,y) of two integers satisfying $\gcd(a,b) = xa + yb$.

For instance, a Bezout pair for $(4,7)$ is a pair (x,y) of integers satisfying $\gcd(4,7) = x \cdot 4 + y \cdot 7$. In view of $\gcd(4,7) = 1$, this latter equation simplifies to $1 = 4x + 7y$. So a Bezout pair for $(4,7)$ is a solution to this equation $1 = 4x + 7y$ in **integers** x and y. This is similar to the coin problem from §1.9.1 (in Lecture 5), in the sense that you can think of such a Bezout pair (x,y) as a way to pay 1 cent with x many 4-cent coins and y many 7-cent coins, assuming that you are allowed to get change (because x and y are allowed to be negative). Without change, of course, you could not pay 1 cent using 4-cent coins and 7-cent coins. But with change, it works: You pay two 4-cent coins and get one 7-cent coin in return, and thus end up paying $2 \cdot 4 + (-1) \cdot 7 = 1$ cent, which is what you wanted. In other words, the pair $(x,y) = (2,-1)$ satisfies $1 = 4x + 7y$. In other words, $(2,-1)$ is a Bezout pair for $(4,7)$. There are also other Bezout pairs for $(4,7)$, for example $(-5,3)$ (since $4(-5) + 7 \cdot 3 = 1$). So a Bezout pair is usually not unique.

So Bezout's theorem can be restated as follows: For any two integers a and b, you can pay $\gcd(a,b)$ cents with a-cent coins and b-cent coins, if you can get change[3]. What denominations can be paid **without** change is a more complicated story, and we will return to this in §3.8 (Lecture 11).

[3] more precisely: if you can get change in a-cent coins and b-cent coins (and there are infinitely many coins of either denomination available)

Here is another example: A Bezout pair for $(6, 16)$ is $(3, -1)$, since $\gcd(6, 16) = 2 = 6x + 16y$ for $(x, y) = (3, -1)$.

So Bezout's theorem (Theorem 3.4.6) is saying that for any two integers $a, b \in \mathbb{Z}$, there exists a Bezout pair for (a, b).

How can we prove this theorem? Induction (particularly strong induction) appears to be a reasonable method. Unfortunately, induction can only be used to prove a statement about elements of a set of the form $\{k, k+1, k+2, \ldots\}$ for a given integer k (that is, a statement about integers from a given lower bound onwards). To put it differently, induction can only prove a statement that "starts somewhere" (even if it is presented as a strong induction with no base case). Meanwhile, in Bezout's theorem, both a and b are just arbitrary integers, so they can be arbitrarily low.

This hurdle can be surmounted: While we cannot prove Bezout's theorem by induction directly, we can first restrict it to the case when $b \in \mathbb{N}$, and prove this restriction by induction. In other words, we shall use induction to prove the following particular case of Bezout's theorem:

Lemma 3.4.8 (restricted Bezout's theorem)**.** Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then, there exists a Bezout pair for (a, b).

Once this lemma is proved, we will quickly deduce Bezout's theorem in full generality from it. So let us prove this lemma.

Proof of Lemma 3.4.8. We shall use strong induction on b. Here, we do not consider a to be fixed. Thus, the statement that we will be proving for all $b \in \mathbb{N}$ is

$$P(b) := (\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a, b)).$$

Our goal is to prove this statement $P(b)$ for all $b \in \mathbb{N}$. We shall do this by strong induction on b:

Base case: Let us prove the statement $P(0)$. Indeed, for each $a \in \mathbb{Z}$, let us set

$$\operatorname{sign} a := \begin{cases} 1, & \text{if } a > 0; \\ 0, & \text{if } a = 0; \\ -1, & \text{if } a < 0. \end{cases}$$

Then, for each $a \in \mathbb{Z}$, the pair $(\operatorname{sign} a, 0)$ is a Bezout pair for $(a, 0)$, since

$$\begin{aligned} \gcd(a, 0) &= |a| && (\text{by Proposition 3.4.3 } \textbf{(b)}) \\ &= (\operatorname{sign} a) \cdot a && \left(\begin{array}{c}\text{this is a general fact that holds for any real} \\ \text{number } a \text{, and can be easily verified by} \\ \text{checking the cases } a > 0,\ a = 0 \text{ and } a < 0\end{array}\right) \\ &= (\operatorname{sign} a) \cdot a + 0 \cdot 0. \end{aligned}$$

Hence, for each $a \in \mathbb{Z}$, there exists a Bezout pair for $(a, 0)$. In other words, the statement $P(0)$ holds.

Induction step: Fix a positive integer b. We must prove the implication

$$(P(0) \text{ AND } P(1) \text{ AND } P(2) \text{ AND } \cdots \text{ AND } P(b-1)) \Longrightarrow P(b).$$

Thus, we assume (as the induction hypothesis) that $P(0)$ AND $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(b-1)$ holds. In other words, we assume that the b statements $P(0)$, $P(1)$, $P(2)$, $\ldots$, $P(b-1)$ all hold. In other words, we assume that

$$\begin{aligned}
&(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a, 0)) \text{ and} \\
&(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a, 1)) \text{ and} \\
&(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a, 2)) \text{ and} \\
&\cdots \qquad \text{and} \\
&(\text{for each } a \in \mathbb{Z}, \text{ there exists a Bezout pair for } (a, b-1)).
\end{aligned}$$

In other words, we assume that for each $a \in \mathbb{Z}$ and each $d \in \{0, 1, \ldots, b-1\}$, there exists a Bezout pair for (a, d). Renaming a as c here, we can restate this as follows: We assume that for each $c \in \mathbb{Z}$ and each $d \in \{0, 1, \ldots, b-1\}$, there exists a Bezout pair for (c, d). So this is our induction hypothesis (brought to its most convenient form).

Our goal is now to prove $P(b)$. In other words, we must prove that for each $a \in \mathbb{Z}$, there exists a Bezout pair for (a, b).

So we fix an $a \in \mathbb{Z}$, and we set out to find a Bezout pair for (a, b).

The Euclidean recursion (Corollary 3.4.4) yields

$$\gcd(a, b) = \gcd(b,\ a\%b). \tag{1}$$

However, $a\%b \in \{0, 1, \ldots, b-1\}$ (by Proposition 3.3.11 **(a)** from Lecture 8, applied to $n = a$ and $d = b$).

Recall our induction hypothesis, which says that for each $c \in \mathbb{Z}$ and each $d \in \{0, 1, \ldots, b-1\}$, there exists a Bezout pair for (c, d). We can apply this to $c = b$ and $d = a\%b$ (because $b \in \mathbb{Z}$ and $a\%b \in \{0, 1, \ldots, b-1\}$), and thus conclude that there exists a Bezout pair for $(b,\ a\%b)$. Let us denote this Bezout pair by (u, v). Thus, by the definition of a Bezout pair, u and v are integers and satisfy

$$\gcd(b,\ a\%b) = ub + v(a\%b). \tag{2}$$

However, Proposition 3.3.11 **(d)** from Lecture 8 (applied to $n = a$ and $d = b$) yields

$$a = (a//b)\,b + (a\%b).$$

Solving this for $a\%b$, we obtain

$$(a\%b) = a - (a//b)\,b. \tag{3}$$

Now, (1) becomes

$$\begin{aligned}
\gcd(a,b) = \gcd(b,\ a\%b) &= ub + v \underbrace{(a\%b)}_{\substack{=a-(a//b)b \\ \text{(by (3))}}} \qquad \text{(by (2))} \\
&= ub + v\left(a - (a//b)\, b\right) \\
&= ub + va - v\,(a//b)\, b \\
&= \underbrace{v}_{\text{an integer}} a + \underbrace{(u - v\,(a//b))}_{\text{an integer}} b.
\end{aligned}$$

Thus, we have written $\gcd(a,b)$ as a multiple of a plus a multiple of b. More specifically, the pair

$$(v,\ u - v\,(a//b))$$

is a Bezout pair for (a,b). And so we conclude that there exists a Bezout pair for (a,b) (because we just found one). This proves the statement $P(b)$ for our b, and thus completes the induction step.

Hence, by induction, we have shown that $P(b)$ holds for all $b \in \mathbb{N}$. But this is saying precisely that there exists a Bezout pair for (a,b) whenever $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Thus, Lemma 3.4.8 is proved. □

This inductive proof contains a recursive algorithm for finding a Bezout pair for (a,b) whenever $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Written in Python, this algorithm looks as follows:[4]

```
def bezout_pair(a, b):  # for b nonnegative
    if b == 0:
        return (sign(a), 0)
    (u, v) = bezout_pair(b, a%b)
    return (v, u - v * (a//b))
```

This algorithm is known as the **extended Euclidean algorithm**.

Now that Lemma 3.4.8 has been proven, Bezout's theorem in the general case (Theorem 3.4.6) easily follows:

Proof of Theorem 3.4.6. We are in one of the following two cases:

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

[4] Here, sign(a) is what was called sign a in the above proof. In Python, this can be defined as follows:

```
def sign(a):
    if a < 0:
        return -1
    if a == 0:
        return 0
    if a > 0:
        return 1
```

Case 2: We have $b < 0$.

Let us first consider Case 1. In this case, $b \geq 0$. Hence, $b \in \mathbb{N}$. Thus, Lemma 3.4.8 yields that there exists a Bezout pair for (a, b). In other words, there exists a pair (x, y) of two integers satisfying $\gcd(a, b) = xa + yb$ (by the definition of a Bezout pair). But this is precisely what Theorem 3.4.6 is claiming. Thus, Theorem 3.4.6 is proved in Case 1.

Let us now consider Case 2. In this case, $b < 0$. Hence, $-b > 0$, so that $-b \in \mathbb{N}$. Hence, Lemma 3.4.8 (applied to $-b$ instead of b) yields that there exists a Bezout pair for $(a, -b)$. Let (u, v) be this Bezout pair. Then, by the definition of a Bezout pair, u and v are integers and satisfy $\gcd(a, -b) = ua + v(-b)$.

However, Proposition 3.4.3 **(h)** yields $\gcd(a, -b) = \gcd(a, b)$. Thus,

$$\gcd(a,b) = \gcd(a,-b) = ua + \underbrace{v(-b)}_{=(-v)b} = ua + (-v)b.$$

Thus, there exist two integers x and y such that $\gcd(a, b) = xa + yb$ (namely, $x = u$ and $y = -v$). This proves Theorem 3.4.6 in Case 2.

We have now proved Theorem 3.4.6 in both Cases 1 and 2, so that the theorem always holds. □

3.4.5. The universal property of the gcd

Bezout's theorem is helpful for proving properties of gcds. Here is the most important one, which is called the **universal property of the gcd**:

Theorem 3.4.9 (universal property of the gcd)**.** Let $a, b, m \in \mathbb{Z}$. Then, we have the equivalence

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

In other words, the common divisors of a and b are precisely the divisors of $\gcd(a, b)$. In other words, $\gcd(a, b)$ is not just the greatest among the common divisors of a and b (if a and b are not both 0), but it also is divisible by all of them.

Proof of Theorem 3.4.9. We must prove the two implications

$$(m \mid a \text{ and } m \mid b) \implies (m \mid \gcd(a, b))$$

and

$$(m \mid \gcd(a, b)) \implies (m \mid a \text{ and } m \mid b).$$

The second of these two implications is easy to prove: If $m \mid \gcd(a, b)$, then $m \mid a$ (since $m \mid \gcd(a, b) \mid a$) and $m \mid b$ (similarly).

It thus remains to prove the first implication: i.e., to prove that

$$(m \mid a \text{ and } m \mid b) \implies (m \mid \gcd(a,b)).$$

To prove this, we assume that $m \mid a$ and $m \mid b$. We must show that $m \mid \gcd(a,b)$.

Bezout's theorem (Theorem 3.4.6) tells us that there exist two integers x and y such that $\gcd(a,b) = xa + yb$. Consider these x and y. Then, $m \mid a \mid xa$, so that xa is a multiple of m. Similarly, yb is a multiple of m. Thus, $xa + yb$ is a multiple of m as well (since a sum of two multiples of m is again a multiple of m). But this is saying that $\gcd(a,b)$ is a multiple of m (since $\gcd(a,b) = xa + yb$). In other words, $m \mid \gcd(a,b)$. But this is precisely what we wanted to show. Thus, the first implication is proved, and the proof of Theorem 3.4.9 is complete. □