Exercise 1

Let a, b be arbitrary positive integers.

a) If b is a multiple of a, find $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$.

b) Find $\gcd(a, 0)$ and $\operatorname{lcm}(a, 0)$.

c) Find $\gcd(a, 1)$ and $\operatorname{lcm}(a, 1)$.

d) Under what conditions is $\gcd(a, b) = 0$, $\operatorname{lcm}(a, b) = 1$, $\operatorname{lcm}(a, b) = 0$?

e) Find $\gcd(840, -126)$ by running the Euclidean algorithm and, from that, $\operatorname{lcm}(840, -126)$. Do the same using the prime factor decompositions of 840 and 126.

f) Find $\gcd(144, 89)$ and $\operatorname{lcm}(144, 89)$.
Hint: In this particular case there is a faster way than running the Euclidean algorithm.

Solution:

a) $\gcd(a, b) = a$. We verify it by checking the three conditions for the GCD: first, $a \mid a$ (obvious); second, $a \mid b$ (we have this as an assumption); third, if $d \mid a$ and $d \mid b$ then also $d \mid a$ (obvious). Similarly, we find that $\operatorname{lcm}(a, b) = b$.

b) $\gcd(a, 0) = a$ and $\operatorname{lcm}(a, 0) = 0$ are consequences of a) (0 is always a multiple of a).

c) $\gcd(a, 1) = 1$ and $\operatorname{lcm}(a, 1) = a$ are also consequences of a) (a is always a multiple of 1).

d) 0 is the greatest number (with respect to the divisibility order), so $\gcd(a, b) = 0$ happens whenever 0 is a common divisor of a and b. This can only be the case when $a = b = 0$.

Similarly, $\operatorname{lcm}(a, b) = 1$ happens whenever 1 is a multiple of both a and b, which can only be when $a = b = 1$.

Lastly, since 0 is the greatest number (w.r.t. divisibility), it can only be the *least* common multiple of a and b if there are no other common multiple of a and b. Since $a \cdot b$ is always a common multiple of a and b, we must thus have $a \cdot b = 0$. Thus $\operatorname{lcm}(a, b) = 0$ happens if and only if $a = 0$ or $b = 0$ (or both).

e) $\gcd(840, -126) = \gcd(840, 126) = \gcd(84, 126) = \gcd(84, 42) = \gcd(0, 42) = 42$.

Using the formula from the lecture, we now also find that $\operatorname{lcm}(840, -126) = \frac{|840| \cdot |-126|}{42} = 20 \cdot 126 = 2520$.

Alternatively, we could have factored $840 = 2^3 \cdot 3 \cdot 5 \cdot 7$ and $126 = 2 \cdot 3^2 \cdot 7$ and computed $\gcd(840, -126) = \gcd(840, 126) = 2 \cdot 3 \cdot 7 = 42$ and $\operatorname{lcm}(840, -126) = \operatorname{lcm}(840, 126) = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$.

f) 89 is prime, so $\gcd(144, 89) = 89$ if 144 is a multiple of 89 or $\gcd(144, 89) = 1$ otherwise. Clearly, 144 is not a multiple of 89, so we have $\gcd(144, 89) = 1$ and $\operatorname{lcm}(144, 89) = 144 \cdot 89 = 12816$.

Exercise 2

a) Apply the extended Euclidean algorithm to find $\gcd(74, 30)$ and the coefficients u, v from Bézout's lemma. Show your intermediate steps and check your final result.

b) Find the multiplicative inverse of $\overline{39}$ mod 154.

c) Find the two smallest integers n (with $n \geq 2$) such that $\overline{39} \bmod n$ is not invertible.

d) Which of the congruence classes in $\mathbb{Z}/10$ are invertible?

e) Which of the congruence classes in $\mathbb{Z}/60$ are invertible?
Hint: What prime factors can a number $k < 60$ with $\gcd(k, 60) = 1$ contain?

Solution:

a) We compute, in sequence, the triples $(74, 1, 0)$, $(30, 0, 1)$, $(14, 1, -2)$, $(2, -2, 5)$. Now we read off $u = -2$ and $v = 5$ and check that indeed $-2 \cdot 74 + 5 \cdot 30 = 2$. The value 2 as GCD also makes sense because $74 = 2 \cdot 37$ and $30 = 2 \cdot 3 \cdot 5$.

b) We compute the triples: $(39, 1, 0)$, $(154, 0, 1)$, $(39, 1, 0)$, $(37, -3, 1)$, $(2, 4, -1)$, $(1, -75, 19)$. This gives us $u = -75$ and $v = 19$. Thus $\overline{-75} \bmod 154$ is the desired inverse. If we want to normalise this to values between 0 and 153, we can add 154 to obtain $\overline{79}$. We can check the result by computing $(39 \cdot 79) \bmod 154 = 1$.

c) If we want $\overline{39} \bmod n$ to not be invertible, we simply have to find an n such that $\gcd(39, n) \neq 1$. Since 39 factors into the primes 3 and 13, this is the case if and only if n is a multiple of 3 or 13. The two smallest numbers that satisfy this are 3 and 6.

d) We have $\mathbb{Z}_{10} = \{\overline{0}, \ldots, \overline{9}\}$. We have to figure out which of these are coprime to 10. Obviously, the even ones (i.e. $\overline{k}$ with k even) are not coprime to 10 because they share the factor 2. Of course, $\overline{5}$ is also not coprime to 10 because 5 divides 10. All the remaining ones are indeed coprime, i.e. $\overline{1}, \overline{3}, \overline{7}, \overline{9}$.

e) 60 numbers is a bit much for a brute force search, so let us try something more clever.

For a number to be coprime to 60 it must not share any prime factors with 60, i.e. the prime factors $2, 3, 5$ are not allowed. Because we need numbers less than 60, the only prime factors that can occur are then $7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59$. These are all coprime to 60.

We now have to look at numbers that contain more than one of these allowed prime factors (or the same one more than once). It is easy to see that the only combination that gives us a number less than 60 is $7 \cdot 7 = 49$.

Lastly, there is also the number 1, which contains no prime factors and is always invertible.

In conclusion, the invertible congruence classes are:

$$\overline{1},\ \overline{7},\ \overline{11},\ \overline{13},\ \overline{17},\ \overline{19},\ \overline{23},\ \overline{29},\ \overline{31},\ \overline{37},\ \overline{41},\ \overline{43},\ \overline{47},\ \overline{49},\ \overline{53},\ \overline{59}$$

This also agrees with what Euler's totient function tells us: $\varphi(60) = \varphi(2^2) \cdot \varphi(3) \cdot \varphi(5) = 16$, so there have to be 16 invertible congruence classes modulo 60.

Exercise 3

a) Show that the coefficients from by Bézout's Theorem are 'optimal' in the sense that it is not possible to achieve a 'smaller' number than $\gcd(a, b)$ with linear combinations of a and b.

Formally: Show that for any $a, b, u, v \in \mathbb{Z}$ we have $\gcd(a, b) \mid ua + vb$.

b) Using a), how could you quickly convince somebody that a and b are coprime if that person is not willing to run Euclid's algorithm themselves?

c) How could you convince them that $\gcd(a, b)$ has some particular value? You may use the results from the Bonus exercise.

Solution:

a) Define $d := \gcd(a, b)$ and write $a = da'$ and $b = db'$. We have $ua + vb = uda' + vdb' = (ua' + vb') \cdot d$. This proves that $ua + vb$ is a multiple of d.

b) We can certify that a, b are coprime by computing u, v with $ua + vb = 1$ using Bézout's Theorem. Because of a), just knowing that $ua + vb = 1$ means that $\gcd(a, b) \mid 1$, which clearly implies that $\gcd(a, b) = 1$. Thus if we provide u, v to the other person, they can simply check $ua + vb = 1$.

Note however that this is, algorithmically speaking, not really faster than just running Euclid's algorithm – so its usefulness is limited.

c) For $d = 0$ it is obvious, since $\gcd(a, b) = d$ iff $a = b = 0$.

Otherwise, if we want to convince them that $\gcd(a, b) = d$ then they can first check that $d > 0$ and $d \mid a$ and $d \mid b$. If this is the case, they can compute $a' := a/d$ and $b' := b/d$. Now, $\gcd(a, b) = \gcd(da', db') = |d| \cdot \gcd(a', b') = d \cdot \gcd(a', b')$. Thus if we want to convince them that $\gcd(a, b) = d$, we now still need to convince them that $\gcd(a', b') = 1$ – but we already know how to do that from Exercise b).

In summary, to make things as easy as possible, we can convince the person that $\gcd(a, b) = d$ by providing them with a triple (a', b', u, v) such that $a = da'$ and $b = db'$ and $ua' + vb' = 1$.

Bonus exercise

a) Prove that $\gcd(ca, cb) = |c| \cdot \gcd(a, b)$. **Hint:** Use prime factor decompositions of a, b, c.

b) Let $a, b \in \mathbb{Z}$ be integers that are not both 0. Using a), show that $a/\gcd(a, b)$ and $b/\gcd(a, b)$ are coprime.

Solution:

a) We assume w.l.o.g. that a, b, c are all positive numbers. If one of them is 0 the theorem becomes trivial; if all of them are non-zero and some of them negative we can simply take the absolute value to make them all positive.

Let $p_1, \dots, p_k$ be all the primes that occur as factors in a, b, or c and e_i, f_i, g_i their respective multiplicities in a, b, c. That is, $a = \prod_{i=1}^k p_i^{e_i}$ and $b = \prod_{i=1}^k p_i^{f_i}$ and $c = \prod_{i=1}^k p_i^{g_i}$.

The prime factor decompositions of ca and cb are $ca = \prod_{i=1}^k p_i^{e_i+g_i}$ and $cb = \prod_{i=1}^k p_i^{f_i+g_i}$. Thus:

$$\begin{aligned}\gcd(ca, cb) &= \prod_{i=1}^k p_i^{\max(e_i+g_i, f_i+g_i)} = \prod_{i=1}^k p_i^{\max(e_i, f_i)+g_i} \\ &= \left(\prod_{i=1}^k p_i^{\max(e_i, f_i)}\right) \cdot \left(\prod_{i=1}^k p_i^{g_i}\right) = \gcd(a, b) \cdot c\end{aligned}$$

Note: A direct proof based only on the characteristic properties of gcd is also possible but somewhat more complicated.

b) Let $d := \gcd(a, b)$ and write $a := da'$ and $b := db'$. Note that $d > 0$ because a and b are not both zero. Our objective is to show that a' and b' are coprime.

We have $d \overset{\text{def}}{=} \gcd(a, b) \overset{\text{def}}{=} \gcd(da', db') \overset{\text{a)}}{=} |d| \cdot \gcd(a', b') = d \cdot \gcd(a', b')$. Cancelling d, we obtain $\gcd(a', b') = 1$.