Elementary Number Theory - Exercise 1b

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. Let $a, b, n \in \mathbb{N}$ be natural numbers.

1. What is $\gcd(n,0), \gcd(n,1), \gcd(n,n), \gcd(n,2n)$?
2. Show that $\gcd(a, a+b) = \gcd(a,b)$.
3. Show that $\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) = 1$.

Solution 1.

1. We have
$$\gcd(n,0) = \max\{d \in \mathbb{N} : d \mid n,\, d \mid 0\} = \max\{d \in \mathbb{N} : d \mid n\} = n.$$
Similarly, we find $\gcd(n,1) = 1$, $\gcd(n,n) = n$, and $\gcd(n,2n) = n$.

2. If $d \mid \gcd(a, a+b)$, then $d \mid a$ and $d \mid a+b$. This implies $d \mid b$, so $d \mid \gcd(a,b)$. Conversely, if $d \mid \gcd(a,b)$ then $d \mid a$ and $d \mid b$, so $d \mid a+b$, hence $d \mid \gcd(a, a+b)$. This shows $\gcd(a, a+b) = \gcd(a,b)$.

3. By Bezout's Lemma we can find $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a,b)$. Dividing by $\gcd(a,b)$ gives
$$\frac{a}{\gcd(a,b)}x + \frac{b}{\gcd(a,b)}y = 1,$$
which implies that $\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) = 1$ (since otherwise $\frac{a}{\gcd(a,b)}x + \frac{b}{\gcd(a,b)}y$ would be divisible by this gcd, but 1 is not).

Problem 2.

1. Show that $\gcd(n, n+1) = 1$ for any $n \in \mathbb{Z}$.
2. Show that $\gcd(22n+7, 33n+10) = 1$ for any $n \in \mathbb{Z}$.

Solution 2.

1. We have $-n + (n+1) = 1$. Now $\gcd(n, n+1)$ divides the left-hand side, so it divides 1, which implies $\gcd(n, n+1) = 1$.

2. We want to find integers x, y such that
$$(22n+7)x + (33n+10)y = 1.$$
It might be a good idea to try to cancel out $22n$ with $33n$, so we put $x = 3s$ and $y = -2t$. Then the equation becomes
$$7 \cdot (3s) + 10 \cdot (-2t) = 1$$
or in other words
$$21s - 20t = 1.$$
This equation is satisfied by $s = t = 1$. Hence, we put $x = 3$ and $y = -2$, and compute
$$(22n+7) \cdot 3 + (33n+10) \cdot (-2) = 7 \cdot 3 + 10 \cdot (-2) = 1,$$
which shows that $\gcd(22n+7, 33n+10) = 1$.

Problem 3. Show that, for $a = bq + r$, we have $\gcd(a, b) = \gcd(b, r)$. Use this to convince yourself that the Euclidean Algorithm really computes $\gcd(a, b)$.

Solution 3. It suffices to show that any divisor of a and b also divides b and r, and vice versa. So let $d \mid a, d \mid b$. Then $a = bq + r$ means $r = a - bq$, which shows $d \mid r$. The converse direction is analogous.

Recall that the Euclidean Algorithm does division with remainder as follows:

$$\begin{aligned} a &= bq_1 + r_1 && (0 \leq r_1 < |b|), \\ b &= q_2 r_1 + r_2 && (0 \leq r_2 < r_1), \\ r_1 &= q_3 r_2 + r_3 && (0 \leq r_3 < r_2), \\ &\vdots \\ r_{n-1} &= r_n q_{n+1} + \underbrace{r_{n+1}}_{=0}. \end{aligned}$$

The output is r_n, and we want to show that this is equal to $\gcd(a, b)$. By what we have shown in this problem, we have

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_n, r_{n+1}) = r_n,$$

so the Euclidean Algorithm indeed computes $\gcd(a, b)$.

Problem 4. Compute $\gcd(90, 14)$ and $x, y \in \mathbb{Z}$ with $90x + 14y = \gcd(90, 14)$ using the Euclidean Algorithm.

Solution 4. We apply the Euclidean Algorithm and do division with remainder:

$$\begin{aligned} 90 &= 6 \cdot 14 + 6 \\ 14 &= 2 \cdot 6 + 2 \\ 6 &= 3 \cdot 2, \end{aligned}$$

so $\gcd(90, 14) = r_2 = 2$. In order to compute x, y, we compute

$$\begin{aligned} x_0 = 0, &\quad y_0 = 1, \\ x_1 = 1, &\quad y_1 = -6, \\ x_2 = 0 - 2 \cdot 1 = -2, &\quad y_2 = 1 - 2 \cdot (-6) = 13, \end{aligned}$$

so we find $x = -2, y = 13$. Indeed, we have $90 \cdot (-2) + 14 \cdot 13 = 2$.

Problem 5. (Homework) The Fibonacci numbers F_n are defined recursively via $F_0 = 0, F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. The first few F_n are given by $0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$.

1. Show that
$$\gcd(F_n, F_{n+1}) = 1, \qquad \text{for all } n \in \mathbb{N}.$$

2. Prove *Honsberger's identity*

$$F_{m+n} = F_m F_{n+1} + F_{m-1} F_n, \qquad \text{for all } m, n \in \mathbb{N}.$$

3. Show that $m \mid n$ implies that $F_m \mid F_n$.

Solution 5. 1. For $n = 1$ we have $F_1 = 1$ and $F_2 = 1$, so $\gcd(F_1, F_2) = 1$. For $n > 1$ we apply the recursion to see that

$$\gcd(F_n, F_{n+1}) = \gcd(F_n, F_n + F_{n-1}) = \gcd(F_n, F_{n-1}),$$

where we used the general formula $\gcd(a, a + b) = \gcd(a, b)$. Now the claim follows by induction.

2. For fixed $n \in \mathbb{N}$ we consider the claim

$$P(n): \quad F_{m+n} = F_{m-1} F_n + F_m F_{n+1} \qquad \text{for all } m \in \mathbb{N},$$

and prove $P(n)$ by induction on n. The cases $P(1)$ and $P(2)$ can be checked directly, using the recursive definition of the definition numbers. These are the base cases of the induction.

Let us assume that $P(k)$ holds for all $k \leq n$, for some fixed $n \geq 2$. We need to check that $P(n + 1)$ holds. For any $m \in \mathbb{N}$ we can now compute

$$\begin{aligned} F_{m+n+1} &= F_{m+n} + F_{m+n-1} && \text{(Definition of Fibonacci numbers)} \\ &= (F_{m-1} F_n + F_m F_{n+1}) + F_{m-1} F_{n-1} + F_m F_n && (P(n) \text{ and } P(n-1)) \\ &= F_{m-1}(F_n + F_{n-1}) + F_m(F_{n+1} + F_n) \\ &= F_{m-1} F_{n+1} + F_m F_{n+2} && \text{(Definition of Fibonacci numbers)}, \end{aligned}$$

which proves $P(n + 1)$.

3. Let us look at Honsberger's identity

$$F_{m+n} = F_m F_{n+1} + F_{m-1} F_n.$$

Since the first summand $F_m F_{n+1}$ is divisible by F_m, we see that $F_m \mid F_n$ implies that $F_m \mid F_{n+m}$, for any n. In particular, since $F_m \mid F_m$, we get that

$$F_m \quad \text{divides} \quad F_m,\ F_{2m},\ F_{3m},\ F_{4m}, \ldots$$

that is, $F_m \mid F_{km}$ for all $k \in \mathbb{N}$. In other words, we have $F_m \mid F_n$ whenever $m \mid n$.

Problem 6. (Homework)

1. Find three integers which are coprime, but not pairwise coprime.

2. For any given r, find a sequence $a_1, a_2, \ldots, a_r$ of r integers which are coprime (that is, $\gcd(a_1, \ldots, a_r) = 1$), such that any $r - 1$ elements of the sequence are not coprime.
Remark: The numbers $a_1, \ldots, a_r$ need not be *pairwise* coprime.

Solution 6. 1. For example, $1, 2, 4$ are coprime, but not pairwise coprime. Note that 1 is of course coprime to 2 and 4, but 2 and 4 are not coprime. In particular, if a sequence of integers is not pairwise coprime, it may still be that *some* numbers in the sequence are not coprime to each other.

2. Let $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ be the sequence of prime numbers. For $j \in \{1, \ldots, r\}$ consider the product

$$a_j = \prod_{\substack{i=1 \\ i \neq j}}^{r} p_i$$

of all the primes $p_1, \ldots, p_r$ apart from p_j. Then the a_j are coprime, since each a_j (hence their gcd) is at most divisible by the primes $p_1, \ldots, p_r$, but p_j does not divide a_j. However, if we take $r - 1$ elements from the sequence, then exactly one a_j is missing, so our $r - 1$ elements are all divisible by the prime p_j.

Problem 7 (sage)**.** Implement the following functions in sage:

1. `divide(a,b)`: compute q, r such that $a = bq + r$ and $0 \leq r < |b|$.
2. `gcd(a,b)`: compute $\gcd(a, b)$ using the Euclidean Algorithm.
3. `bezout(a,b)`: compute integers x, y such that $ax + by = \gcd(a, b)$.