September 9, 2024

**Problem Set 1 Solutions**

**Exercise 1.** *Use the fundamental theorem of arithmetic and the well-ordering principle to show that for a prime number $p$, the square root $\sqrt{p}$ is irrational.*

**Solution 1.** Assume to the contrary, that there exist $a, b \in \mathbb{Z}^+$ such that $\sqrt{p} = \frac{a}{b}$. By the well-ordering principle, of all such couples $(a, b)$ we can choose the one where $a$ is the least element. Then $a$ and $b$ are relatively prime. Then $p = \frac{a^2}{b^2}$, so $pb^2 = a^2$. By the unique factorisation in $\mathbb{Z}^+$, we have that $p$ divides $a$. So $a = pk$ for some $k \in \mathbb{Z}^+$. So $pb^2 = (pk)^2 = p^2k^2$ and we have $b^2 = pk^2$. Again by the unique factorisation, we see that $p$ divides $b$, which contradicts the choice of $(a, b)$ where $a$ is the least element, and therefore $a$ and $b$ have no common divisor. Hence $\sqrt{p}$ is not rational.

**Exercise 2.** *Show that the strong induction principle implies the well ordering principle.*
*Strong induction principle: Let $P(n)$ be a statement that depends on $n \in \mathbb{N}$. If*

1. *$P(0)$ is true, and*
2. *$\{P(0), P(1), \dots P(n)\}$ imply $P(n+1)$ for any $n \in \mathbb{N}$,*

*then $P(n)$ is true for all $n \in \mathbb{N}$.*

**Solution 2.** Suppose to the contrary that there exists a nonempty subset $Y \subset \mathbb{N}$ that contains no least element. Let $P(n)$ be the statement "$n \notin Y$".
Base: If $0 \in Y$, then 0 is the least element because it is the least element in $\mathbb{N}$. Therefore $0 \notin Y$ and $P(0)$ is true.
Induction step: Suppose that for some $n \in \mathbb{N}$, $\{P(0), P(1), \dots P(n)\}$ are true. This means that none of the numbers $0, 1, \dots n$ are in $Y$. Then if $(n+1) \in Y$, it is the least element in $Y$. Therefore, $(n+1) \notin Y$ and $P(n+1)$ is true.
Conclusion: By the strong induction, for all $n \in \mathbb{N}$ we have $n \notin Y$. But $Y$ is a nonempty subset of $\mathbb{N}$, contradiction.

**Exercise 3.** *Use the Euclidean algorithm to find the greatest common divisor $\gcd(a, b)$ for the following integers:*

*(a) $a = 73$ and $b = 12$.*

*(b) $a = 101$ and $b = -32$.*

*(c) $a = 9050$ and $b = 1004$.*

*In each case find integers $x, y \in \mathbb{Z}$ such that $xa + yb = \gcd(a, b)$.*

**Solution 3.** (a) By the Euclidean algorithm we have:

$$73 = 6 \cdot 12 + 1$$
$$12 = 12 \cdot 1 + 0.$$

So the greatest common divisor of 73 and 12 is 1.

Reversing the same algorithm we find:

$$1 = 73 - 6 \cdot 12 = 1 \cdot 73 + (-6)12.$$

Therefore we have $(x, y) = (1, -6)$.

(b) By the Euclidean algorithm we have:

$$\begin{aligned} 101 &= -3 \cdot (-32) + 5 \\ -32 &= -7 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

So the greatest common divisor of 101 and $-32$ is 1.

Reversing the same algorithm we find:

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 = -32 + 7 \cdot 5 - (5 - 1 \cdot 3) \\ &= -32 + 6(101 + 3 \cdot (-32)) + (-32 + 7 \cdot 5) \\ &= 6 \cdot 101 + 20 \cdot (-32) + 7(101 + 3 \cdot (-32)) \\ &= 13 \cdot 101 + 41 \cdot (-32). \end{aligned}$$

Therefore we have $(x, y) = (13, 41)$.

We can arrive at the same result running the Euclidean algorithm for 101 and $32 = |-32|$:

$$\begin{aligned} 101 &= 3 \cdot 32 + 5 \\ 32 &= 6 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Reversing the algorithm we find:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = (101 - 3 \cdot 32) - 2 \cdot (32 - 6 \cdot 5) \\ &= 101 - 3 \cdot 32 - 2 \cdot 32 + 12 \cdot (101 - 3 \cdot 32) \\ &= 13 \cdot 101 - 41 \cdot 32 \\ &= 13 \cdot 101 + 41 \cdot (-32). \end{aligned}$$

Therefore we have as before $(x, y) = (13, 41)$.

(c) $9050 = 1004 \cdot 9 + 14$

$1004 = 14 \cdot 71 + 10$

$14 = 10 \cdot 1 + 4$

$10 = 4 \cdot 2 + 2$

$4 = 2 \cdot 2 + 0$, and so the greatest common divisor of 9050 and 1004 is 2.

To find $x$ et $y$ such that $9050x + 1004y = 2$, we consider the reverse algorithm:

$2 = 10 - 4 \cdot 2$

$= 10 - (14 - 10) \cdot 2 = 3 \cdot 10 - 2 \cdot 14$

$= 3(1004 - 14 \cdot 71) - 2 \cdot 14 = 3 \cdot 1004 - 215 \cdot 14$

$= 3 \cdot 1004 - 215(9050 - 1004 \cdot 9) = 1938 \cdot 1004 - 215 \cdot 9050$. Therefore we have $(x, y) = (-215, 1938)$.

**Exercise 4.** *1. Show that if $a, b \in \mathbb{Z}^*$ and $d = \gcd(a, b)$, then the equation*

$$ax + by = c$$

*has a solution in integer numbers* if and only if $c \in d\mathbb{Z}$.

2. *Suppose that $a, b \in \mathbb{Z}^*$ and $c \in \mathbb{Z}$ are such that the equation $ax+by = c$ has a solution $(x_0, y_0)$ in integer numbers. Find all possible pairs of integer solutions $(x, y)$ in terms of $x_0, y_0, a, b$.*

**Solution 4.** 1. $\Rightarrow$). Since $d|a$ and $d|b$, the equation implies that $d|c$ and therefore $c \in d\mathbb{Z}$.
$\Leftarrow$). By the Euclidean algorithm, there exist $x_1, y_1 \in \mathbb{Z}$ such that

$$ax_1 + by_1 = d.$$

If $c = dk$, $k \in \mathbb{Z}$, multiplying the equation by $k$ gives

$$akx_1 + bky_1 = dk = c.$$

Therefore, $(x, y) = (kx_1, ky_1)$ is a solution.

2. If $(x_0, y_0)$ is a solution of the equation $xa + yb = c$, the fact that $(x, y)$ is another solution of the same equation is equivalent to the statement:

$$(x - x_0)a = (y_0 - y)b.$$

Since $d = \gcd(a, b)$, both sides are divisible by $d$:

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y).$$

Now since $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime, we have $\frac{b}{d} \mid (x - x_0)$ and $\frac{a}{d} \mid (y_0 - y)$. Dividing the equation by $\frac{a}{d} \cdot \frac{b}{d}$, we obtain an integer $k$:

$$\frac{x - x_0}{b/d} = \frac{y_0 - y}{a/d} = k \in \mathbb{Z}.$$

Finally, we have that for any $k \in \mathbb{Z}$ the pair $x = x_0 + k\frac{b}{d}$ and $y = y_0 - k\frac{a}{d}$ provides a solution:

$$a\left(x_0 + k\frac{b}{d}\right) + b\left(y_0 - k\frac{a}{d}\right) = c \qquad \forall k \in \mathbb{Z}.$$

Since all implications are equivalences, these are all possible solutions.

**Exercise 5.** *Bézout's theorem states that two integers $s$ and $t$ are coprime if and only if there exist two integers $x$ and $y$ such that $xs + yt = 1$. Use Bézout's theorem to show that if an integer $n$ divides a product of two integers $a$ and $b$, and $n$ is coprime with $a$, then $n$ divides $b$.*

**Solution 5.** We know that $a$ and $n$ are coprime. Therefore, by Bézout's theorem there exist two integers $x$ and $y$ such that

$$xa + yn = 1.$$

Multiply the obtained equality by the integer $b$:

$$xab + ynb = b.$$

Since $n$ divides the product $ab$, we can write $ab = nk$ for an integer $k$. Then

$$xnk + ynb = n(xk + yb) = Mn = b,$$

where $M = xk + yb$ is an integer. This implies by definition that $n$ divides $b$.