## Homework 3 - solution

1. Find all integer solutions of the equation
a) $12 x-52 y=16$
b) $512 x+355 y=6$

In (a), you might get confused by the minus sign at the $y$-term. For the first step - performing the Euclid's algorithm, you can just ignore it:

$$
\begin{aligned}
& 52=4 \cdot 12+4 \\
& 12=3 \cdot 4
\end{aligned}
$$

So, $\operatorname{gcd}(52,12)=4$. We also immediatelly get $4=52-4 \cdot 12$, and multiplying by 4 , we get

$$
16=4 \cdot 52-16 \cdot 12
$$

So, one of the solutions is $x=-16, y=-4$. By our theorem, we get all the others as $x=-16-13 k$, $y=-4-3 k, k \in \mathbb{Z}$. Actually, we can slightly simplify it by shifting $k \mapsto-(k+1)$ as $x=-3+13 k$, $y=-1+3 k, k \in \mathbb{Z}$.

Let's have a look on (b) starting again with the Euclid's algorithm

$$
\begin{aligned}
512 & =1 \cdot 355+157 \\
355 & =2 \cdot 157+41 \\
157 & =3 \cdot 41+34 \\
41 & =1 \cdot 34+7 \\
34 & =4 \cdot 7+6 \\
7 & =1 \cdot 6+1 \\
6 & =6 \cdot 1
\end{aligned}
$$

So, $\operatorname{gcd}(512,355)=1$, which might have been obvious (since 512 is a power of two and 355 is odd), but we use this also to solve the equation $512 x_{0}+355 y_{0}=1$.

$$
1=7-6=-34+5 \cdot 7=5 \cdot 41-6 \cdot 34=-6 \cdot 157+23 \cdot 41=23 \cdot 355-52 \cdot 157=-52 \cdot 512+75 \cdot 355
$$

Multiplying this by 6 , we get

$$
6=312 \cdot 512+450 \cdot 355
$$

So, we have got a solution $x=312, y=450$. By theorem from the lecture, we get all the other solutions as $x=-312+355 k, y=450-512 k, k \in \mathbb{Z}$. Shifting $k \mapsto k+1$, we can simplify it to $x=43+355 k, y=-62-512 k, k \in \mathbb{Z}$.

By the way, we could have computed the last part in a simpler way. Notice that during the Euclid's algorithm, the number 6 appeared as one of the remainders. So, we could have directly computed

$$
6=34-4 \cdot 7=-4 \cdot 41+5 \cdot 34=5 \cdot 157-19 \cdot 41=-19 \cdot 355+43 \cdot 157=43 \cdot 512-62 \cdot 355
$$

So, we directly get the particular solution $x=43, y=-62$ and hence the general one is $x=43+355 k$, $y=-62-512 k, k \in \mathbb{Z}$.

