MTH 505: Number Theory **Spring 2020**
Homework 1 **Drew Armstrong**

Problem 1. Find the complete integer solution $x, y \in \mathbb{Z}$ to the following Diophantine equation:

$$1035x + 644y = 299.$$

Consider the set of integer vectors (x, y, z) satisfying $1035x + 644y = z$. Beginning with the obvious triples $\mathbf{r}_1 := (1, 0, 1035)$ and $r_2 := (0, 1, 644)$, we perform a sequence of elementary operations corresponding to the Euclidean algorithm:

x	y	z	
1	0	1035	$\mathbf{r}_1$
0	1	644	$\mathbf{r}_2$
1	-1	391	$\mathbf{r}_3 = \mathbf{r}_1 - 1\mathbf{r}_2$
-1	2	253	$\mathbf{r}_4 = \mathbf{r}_2 - 1\mathbf{r}_3$
2	-3	138	$\mathbf{r}_5 = \mathbf{r}_3 - 1\mathbf{r}_4$
-3	5	115	$\mathbf{r}_6 = \mathbf{r}_4 - 1\mathbf{r}_5$
5	-8	23	$\mathbf{r}_7 = \mathbf{r}_5 - 1\mathbf{r}_6$
-28	45	0	$\mathbf{r}_8 = \mathbf{r}_6 - 5\mathbf{r}_7$

In particular, we see that $\gcd(1035, 644) = 23$, and we note that $299 = 23 \cdot 13$. From theorems in the notes, we conclude that the complete solution is given by the linear combinations $13\mathbf{r}_7 + k\mathbf{r}_8 = (15 - 28k, -24 + 45k, 23)$ for all $k \in \mathbb{Z}$:

$$1035(15 - 28k) + 644(-24 + 45k) = 23.$$

Problem 2. Let $a, b, c, k \in \mathbb{Z}$ be any integers satisfying $a = bk + c$. In this case prove that

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

[Hint: Show that the sets of common divisors are the same: $\mathrm{Div}(a, b) = \mathrm{Div}(b, c)$. It follows that the greatest element of each set is the same.]

To prove that the sets $\mathrm{Div}(a, b)$ and $\mathrm{Div}(b, c)$ are the same we must show (1) that $\mathrm{Div}(a, b) \subseteq \mathrm{Div}(b, c)$ and (2) $\mathrm{Div}(b, c) \subseteq \mathrm{Div}(a, b)$.

(1): Consider any element $d \in \mathrm{Div}(a, b)$. By definition this means that $a = da'$ and $b = db'$ for some integers $a', b' \in \mathbb{Z}$. But then we also have

$$c = a - bk = da' - db'k = d(a' - b'k),$$

which implies that $d|c$ and hence $d \in \mathrm{Div}(b, c)$.

(2): Consider any element $d \in \mathrm{Div}(b, c)$. By definition this means that $b = db'$ and $c = dc'$ for some integers $b', c' \in \mathbb{Z}$. But then we also have

$$a = bk + c = db'k + dc' = d(b'k + c'),$$

which implies that $d|a$ and hence $d \in \mathrm{Div}(a, b)$.

Problem 3. In this problem you will give a **non-constructive** proof of Bézout's identity. Consider two nonzero integers $a, b \in \mathbb{Z}$ and define the set

$$S = \{ax + by : x, y \in \mathbb{Z} \text{ and } ax + by > 0\}.$$

This set is non-empty because it contains $|a|$, hence it has a least element by well-ordering. Let $d \in S$ denote this least element.

(a) Prove that d is a common divisor of a and b. [Hint: Let r be the remainder of a mod d. If $r \neq 0$ show that r is an element of S that is smaller than d.]

(b) Continuing from (a), show that d is the **greatest** common divisor of a and b. [Hint: Let e be any common divisor of a and b. Use (a) to show that $e \leqslant d$.]

(a): By definition of d we know that $d = ax + by > 0$ for some integers $x, y \in \mathbb{Z}$. Since $d \neq 0$ we may divide a by d to obtain $a = qd + r$ for some integers $q, r \in \mathbb{Z}$ satisfying $0 \leqslant r < d$. We will show that $r = 0$ and hence $d|a$. So let us assume for contradiction that $r > 0$. Then since

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy) = a(\text{some integer}) + b(\text{some integer})$$

we find that r is an element of S that is strictly smaller than d. Contradiction. A similar argument shows that $d|b$.

(b): Suppose that $e \in \mathbb{Z}$ satisfies $e|a$ and $e|b$. Say $a = ea'$ and $b = eb'$ for some integers $a', b' \in \mathbb{Z}$. Then since $d = ax + by$ we have

$$d = ax + by = ea'x + eb'y = e(a'x + b'y).$$

Finally, since $e|d$ and $d > 0$ we conclude that $e \leqslant d$ as desired.

Combining (a) and (b) shows that $d = \gcd(a, b)$. In particular, we have proved that there exist integers $x, y \in \mathbb{Z}$ satisfying $ax + by = \gcd(a, b)$. This is called Bézout's Identity.

Problem 4. Consider any non-zero integers $a, b, c \in \mathbb{Z}$. In class I defined the greatest common divisor $\gcd(a, b, c)$ as the greatest element of the following set of common divisors:

$$\mathrm{Div}(a, b, c) = \{d \in \mathbb{Z} : d|a \text{ and } d|b \text{ and } d|c\}.$$

Prove that the same concept can also be defined recursively, as follows:

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

[Hint: This comes down to the fact that any common divisor of a and b is a divisor of $\gcd(a, b)$, which can be proved using Bézout's identity.]

Let's say that $d := \gcd(a, b)$ with $a = da'$ and $b = db'$. Following the idea in Problem 2, we will prove that the sets $\mathrm{Div}(a, b, c)$ and $\mathrm{Div}(d, c)$ are the same.

(1): First we assume that $e \in \mathrm{Div}(d, c)$, so that $e|d$ and $e|c$. Let's say $d = ed'$. But then we have $a = da' = ed'a'$ and $b = db' = ed'b'$, which implies that $e|a$ and $e|b$. In summary, we have shown that $e \in \mathrm{Div}(a, b, c)$.

(2): Conversely, suppose that we have $e \in \mathrm{Div}(a, b, c)$ with $a = ea''$, $b = eb''$ and $c = ec''$. Our goal is to show that $e|d$ and hence $e \in \mathrm{Div}(d, c)$. But we know from Bézout's Identity (Problem 3) that there exist some $x, y \in \mathbb{Z}$ satisfying $ax + by = d$. It follows from this that

$$d = ax + by = ea''x + eb''y = e(a''x + b''y),$$

and hence $e|d$ as desired.

Problem 5. Euclid's Lemma. For any integers $a, b, c \in \mathbb{Z}$ with $a|bc$ and $\gcd(a, b) = 1$, prove that $a|c$. [Hint: From Bézout's identity we know that $ax + by = 1$ for some $x, y \in \mathbb{Z}$. Multiply both sides by c.]

Since $a|bc$ we have $bc = ak$ for some $k \in \mathbb{Z}$. And from Bézout's Identity we have $ax + by = 1$ for some integers $x, y \in \mathbb{Z}$. Then multiplying both sides by c gives

$$\begin{aligned} ax + by &= 1 \\ c(ax + by) &= c \\ acx + bcy &= c \\ acx + aky &= c \\ a(cx + ky) &= c, \end{aligned}$$

which implies that $a|c$.

Problem 6. Lamé's Theorem. Consider some integers $a, b \in \mathbb{Z}$ with $a > b \geqslant 0$ and suppose that the Euclidean algorithm uses n divisions with remainder to compute $\gcd(a, b)$. In this case, Lamé's Theorem says that we must have $a \geqslant F_{n+1}$ and $b \geqslant F_n$, where the Fibonacci numbers are defined by $F_0 = 0$, $F_1 = 1$ and $F_m = F_{m-1} + F_{m-2}$.

(a) Prove Lamé's Theorem by induction on n, starting with $n = 0$ and $n = 1$.

(b) Prove by induction that for all $n \geqslant 2$ we have

$$F_n \geqslant \phi^{n-2} = \left(\frac{1 + \sqrt{5}}{2}\right)^{n-2}.$$

(c) Assuming that $n \geqslant 2$, combine parts (a) and (b) to prove that we have $n < 5d + 2$, where d is the number of decimal digits in b.

Before starting the proof, let me first clearly state the Euclidean algorithm. Given a pair (a, b) with $a > b \geqslant 0$ we first define $r_0 := a$ and $r_1 := b$ then for all $r_i \neq 0$ we apply division with remainder to obtain $r_{i-1} = q_{i+1} r_i + r_{i+1}$ and $0 \leqslant r_{i+1} < r_i$. This produces a decreasing sequence of remainders:

$$r_0 > r_1 > r_2 > \cdots > r_n > r_{n+1} = 0.$$

If $r_n > r_{n+1} = 0$ then we say that the algorithm "terminates in n steps." It is not important for this problem, but we also conclude from Problem 2 that

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_n, r_{n+1}) = \gcd(r_n, 0) = r_n.$$

(a): **Base Cases.** If the algorithm terminates in $n = 0$ steps then we must have $b = 0$, in which case $b = 0 \geqslant F_0$ and $a \geqslant 1 = F_1$. If the algorithm terminates in $n = 1$ steps then we must have $b \geqslant 1$ and $a = qb + 0$ for some quotient $q \geqslant 1$, which implies that $b \geqslant 1 = F_1$ and $a \geqslant b + 1 \geqslant 2 \geqslant F_2$.

Induction Step. Now fix some integer $n \geqslant 2$ and let us assume that:

- The Euclidean algorithm applied (a, b) terminates in n steps.
- Lamé's Theorem holds for any pair when the algorithm terminates in $n - 1$ steps.

Let $r_0 = a$ and $r_1 = b$, as in the above discussion. Since the algorithm applied to $(r_0, r_1) = (a, b)$ terminates in n steps it follows that the algorithm applied to $(r_1, r_2) = (b, r_2)$ terminates in $n - 1$ steps. Thus we may assume for induction that $b \geqslant F_n$ and $r_2 \geqslant F_{n-1}$. Finally, since $q_2 > 0$ this implies that

$$a = q_2 b + r_2 \geqslant b + r_2 \geqslant F_n + F_{n-1} = F_{n+1}.$$

(b): We observe that the golden ratio $\phi = (1+\sqrt{5})/2$ satisfies $\phi^2 = \phi + 1$, and hence $\phi^{n+2} = \phi^{n+1} + \phi^n$ for all integers $n \geqslant 0$. Observe that $F_2 = 1 \geqslant 1 = \phi^0$ and $F_3 = 2 \geqslant 1.618 = \phi^1$. Now fix some integer $n \geqslant 4$ and assume for induction that $F_k \geqslant \phi^{k-2}$ for all $2 \leqslant k < n$. It follows that

$$F_n = F_{n-1} + F_{n-2} \geqslant \phi^{n-3} + \phi^{n-4} = \phi^{n-2}.$$

(c): Suppose that the Euclidean algorithm applied to (a, b) terminates in n steps. We showed in part (a) that $b \geqslant F_n$ and we showed in part (b) that $F_n \geqslant \phi^{n-2}$, hence $b \geqslant \phi^{n-2}$. Take the logarithm base 10 of both sides to obtain

$$\begin{aligned} b &\geqslant \phi^{n-2} \\ \log(b) &\geqslant (n-2)\log(\phi) \\ \log(b)/\log(\phi) + 2 &\geqslant n. \end{aligned}$$

We observe that $1/\log(\phi) = 4.785 < 5$. If d is the number of decimal digits in b then we also have $10^{d-1} \leqslant b < 10^d$, which implies that $d - 1 \leqslant \log(b) < d$. It follows that

$$n \leqslant \frac{1}{\log(\phi)} \log(b) + 2 < 5d + 2.$$

[Remark: Maybe this can be improved to $n \leqslant 5d$ with a bit more work.]