MA 541: Modern Algebra I / Fall 2019
Optional challenge problems for homework assignment # 4
Due 10/3/2019 in class

(1) Prove that the well-ordering principle (WOP) and the principle of mathematical induction are equivalent — that is, each implies the other.

(WOP states that any nonempty subset of $\mathbb{Z}^+$ has a least element. Mathematical induction asserts that if a statement is true for $n = 1$, and if you can show that whenever the statement is true for any particular n then it is also true for $n+1$, then the statement is true for all $n \in \mathbb{Z}^+$.)

(2) Euclid's algorithm starts with a pair of (say) positive integers a and b and proceeds to successively divide with remainder:

$$\begin{aligned}
a &= bq + r_1, & 0 &\le r_1 < b \\
b &= r_1 q_2 + r_2, & 0 &\le r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, & 0 &\le r_3 < r_2 \\
&\cdots & &\cdots \\
r_{i-2} &= r_{i-1} q_i + r_i, & 0 &\le r_i < r_{i-1} \\
&\cdots .
\end{aligned}$$

Since $b > r_1 > \cdots > r_i > \cdots \ge 0$, and since the positive integers are well-ordered, eventually some remainder will equal zero. Let r_n be the last nonzero remainder, so that we actually have

$$\begin{aligned}
a &= bq + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
&\cdots \\
r_{n-2} &= r_{n-1} q_n + r_n \\
r_{n-1} &= r_n q_{n+1}
\end{aligned}$$

with

$$0 < r_n < r_{n-1} < \cdots < b.$$

Prove that $r_n = \gcd(a, b)$.

(Hint: First prove that any common divisor of a and b divides each r_i for $i = 1, 2, \cdots n$. Then prove that r_n divides each of $r_{n-1}, r_{n-2}, \cdots, r_2, r_1, b, a$ in turn. Conclude and triumph!)