Math 230 **Spring 2019**
Homework 4 **Drew Armstrong**

Problem 1. Linear Diophantine Equations. Use the Extended Euclidean Algorithm to find all integers $x, y \in \mathbb{Z}$ satisfying the following equation:

$$345x + 234y = 123.$$

Solution. There are several ways to do this. We will use the method from class.

First we use the Euclidean Algorithm to show that $\gcd(345, 234) = 3$:

$$\begin{array}{rcrcr} 345 & = & (1)234 & + & 111 \\ 234 & = & (2)111 & + & 12 \\ 111 & = & (9)12 & + & \boxed{3} \\ 12 & = & (4)3 & + & 0. \end{array}$$

Then we cancel 3 from both sides to obtain the reduced equation, which has the same solution as the original equation:

$$115x + 78y = 41.$$

Since $\gcd(115, 78) = 1$ we know that the general homogeneous solution is $(x, y) = (-78k, 115k)$ for all $k \in \mathbb{Z}$. Next we apply the Extended/Vector Euclidean Algorithm to find one particular solution. That is, we consider the set of triples $(x, y, z) \in \mathbb{Z}^3$ satisfying $115x + 78y = z$. Then we apply the Euclidean Algorithm to the easy triples $\mathbf{r}_1 = (1, 0, 115)$ and $\mathbf{r}_2 = (0, 1, 78)$:

x	y	z	row operation
1	0	115	$\mathbf{r}_1$
0	1	78	$\mathbf{r}_2$
1	-1	37	$\mathbf{r}_3 = \mathbf{r}_1 - (1)\mathbf{r}_2$
-2	3	4	$\mathbf{r}_4 = \mathbf{r}_2 - (2)\mathbf{r}_3$
19	-28	1	$\mathbf{r}_5 = \mathbf{r}_3 - (9)\mathbf{r}_4$
-78	115	0	$\mathbf{r}_6 = \mathbf{r}_4 - (4)\mathbf{r}_5$

To obtain one solution we multiply row $\mathbf{r}_5$ by 41 to get

$$115(19) + 78(-28) = 1$$
$$115(779) + 78(-1148) = 41.$$

Finally, we add the homogeneous solution to obtain the complete solution:

$$115(779 - 78k) + 78(-1148 + 115k) = 41$$
$$345(779 - 78k) + 234(-1148 + 115k) = 123.$$

Problem 2. Euclid's Lemma. For all integers $a, b, c \in \mathbb{Z}$ prove that

$$(a|bc \wedge \gcd(a, b) = 1) \Rightarrow (a|c).$$

[Hint: If $\gcd(a, b) = 1$ then one can use the Extended Euclidean Algorithm to find integers $x, y \in \mathbb{Z}$ satisfying $ax + by = 1$. Multiply both sides of this equation by c.]

Proof. Assume that $a|bc$ (say $ak = bc$ with $k \in \mathbb{Z}$) and $\gcd(a, b) = 1$. From the Extended Euclidean Algorithm there exist integers $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b) = 1$. Now multiply both sides by c to obtain

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

which implies that $a|c$ as desired. □

Problem 3. Prime Numbers. Given integers $d, n \geq 1$ we say that d is a *proper divisor* of n if $d|n$ and $1 < d < n$. An integer $p \geq 2$ is called *prime* if if has no proper divisors.

(a) Prove that every integer $n \geq 2$ has a prime divisor. [Hint: Assume for contradiction that there exists a positive integer with no prime divisor and let m be the smallest such integer. Since m is not prime it must have a proper divisor. Now what?]

(b) **Euclid's Proof of Infinite Primes.** In this problem you will prove that there exist infinitely many prime numbers. So assume for contradiction that there are only finitely many primes, and call them $2 = p_1 < p_2 < \cdots < p_k$. Now consider the number

$$n = (p_1 p_2 \cdots p_k) + 1.$$

From part (a) you know that there exists a prime factor $p|n$. But show that this p cannot be equal to any of $p_1, p_2, \ldots, p_k$.

Proof. (a) Assume for contradiction that there exists some integer $n \geq 2$ that is **not** divisible by any prime number. Let m be the smallest such integer, which exists by Well-Ordering. Since $m|m$ we know that m is not prime. By definition of "prime" there exists a proper divisor $d|m$ with $1 < d < m$. But observe that $d \geq 2$ and $d < m$. Thus by minimality of m there exists a prime number p such that $p|d$. Finally, since $p|d$ and $d|m$ we conclude that $p|m$, which contradicts the fact that m is not divisible by any prime number.

(b) Assume for contradiction that the exist only finitely many primes and call them $2 = p_1 < p_2 < \cdots < p_k$. Now consider the number

$$n = (p_1 p_2 \cdots p_k) + 1.$$

Since $n \geq 2$ we know from part (a) that there exists some prime number p with $p|n$. Say $p\ell = n$ for some $\ell \in \mathbb{Z}$. But then since p is prime we must have $p = p_i$ for some $i \in \{1, \ldots, k\}$ and it follows that

$$\begin{aligned} 1 &= (p_1 \cdots p_k) - n \\ 1 &= p_i \left(p_1 \cdots p_{i-1} p_{i+1} \cdots p_k\right) + p_i k \\ 1 &= p_i \left(p_1 \cdots p_{i-1} p_{i+1} \cdots p_k + \ell\right). \end{aligned}$$

Finally, since $p_i|1$ we conclude that $p_i = \pm 1$, which contradicts the fact that p_i is prime. □

Problem 4. Base-b Arithmetic. Let us fix an integer $b \geq 2$ called the "base."

(a) For all integers $k \geq 1$ observe that $(b-1)(1 + b + b^2 + \cdots + b^{k-1}) = b^k - 1$.

(b) **Existence.** For all integers $n \geq 0$ consider the following statement:

$$P(n) := \text{“}\exists\, r_0, r_1, r_2, \ldots \in \{0, 1, \ldots, b-1\}, n = r_0 + r_1 b + r_2 b^2 + \cdots \text{.”}$$

Fix $n \geq 0$ and assume for induction that $P(n)$ is true. In this case, prove that $P(n+1)$ is also true. [Hint: You have assumed $n = r_0 + r_1 b + r_2 b^2 + \cdots$ for some integers $r_0, r_1, r_2, \ldots \in \{0, 1, \ldots, b-1\}$. Let $k \geq 0$ be the smallest index such that $r_k \neq b-1$ and show that $n+1 = (r_k+1)b^k + r_{k+1}b^{k+1} + r_{k+2}b^{k+2} + \cdots$. You will need part (a).]

(c) **Uniqueness.** For all integers $k \geq 0$ consider the statement $Q(k) :=$ “For all integers $r_0, \ldots, r_k$ and $s_0, \ldots, s_k$ in the set $\{0, 1, \ldots, b-1\}$ we have

$$(r_0 + r_1 b + \cdots + r_k b^k = s_0 + s_1 b + \cdots s_k b^k) \Rightarrow (r_0 = s_0 \wedge r_1 = s_1 \wedge \cdots \wedge r_k = s_k)\text{.”}$$

Fix $k \geq 0$ and assume for induction that $Q(k)$ is true. In this case, prove that $Q(k+1)$ is also true. [Hint: Assume that $n = r_0 + \cdots + r_{k+1}b^{k+1} = s_0 + \cdots + s_{k+1}b^{k+1}$. Now use the fact that the quotient and remainder of n mod b are **unique**.]

Proof. (a) For any integers $b, k \in \mathbb{Z}$ with $k \geq 1$ we have

$$(b-1)(1 + b + b^2 + \cdots + b^{k-1}) = \begin{array}{r} b + b^2 + \cdots + b^{k-1} + b^k \\ -1 - b - b^2 - \cdots - b^{k-1} \end{array} = -1 + b^k.$$

(b) Now fix $b \geq 2$ and consider the statement

$$P(n) := \text{“}\exists\, r_0, r_1, r_2, \ldots \in \{0, 1, \ldots, b-1\}, n = r_0 + r_1 b + r_2 b^2 + \cdots \text{.”}$$

Note that $P(0)$ is true because $0 = 0 + 0b + 0b^2 + \cdots$. Now assume that the statement $P(n)$ is true. That is, assume that there exist integers $r_0, r_1, r_2, \ldots \in \{0, 1, \ldots, b-1\}$ such that

$$n = r_0 + r_1 b + r_2 b^2 + \cdots .$$

In this case we want to prove that there exist $s_0, s_1, s_2, \ldots \in \{0, 1, \ldots, b-1\}$ such that

$$n = s_0 + s_1 b + s_2 b^2 + \cdots .$$

If $r_0 < b-1$ then we can simply add 1 to r_0. But what if $r_0 = b-1$? Then we have to replace r_0 by 0 and “carry the 1.” To deal with all cases at the same time, let $k \geq 0$ be minimal such that $r_k \neq b-1$. Then from part (a) we have

$$\begin{aligned} n &= (b-1) + (b-1)b + \cdots + (b-1)b^{k-1} + r_k b^k + r_{k+1}b^{k+1} + \cdots \\ n &= (b-1)(1 + b + \cdots + b^{k-1}) + r_k b^k + r_{k+1}b^{k+1} + \cdots \\ n &= (-1 + b^k) + r_k b^k + r_{k+1}b^{k+1} + \cdots \\ n+1 &= (r_k+1)b^k + r_{k+1}b^{k+1} + \cdots \\ n+1 &= 0 + 0b + \cdots 0b^{k-1} + (r_k+1)b^k + r_{k+1}b^{k+1} + \cdots . \end{aligned}$$

This prove that $P(n+1)$ is true because $r_k + 1 \leq b_1$.

(c) Next let $Q(k)$ be the statement that “for all integers $r_0, \ldots, r_k$ and $s_0, \ldots, s_k$ in the set $\{0, 1, \ldots, b-1\}$, if $r_0 + r_1 b + \cdots + r_k b^k = s_0 + s_1 b + \cdots + s_k b^k$ then we must have $r_0 = s_0$, $r_1 = r_2$, …and $r_k = s_k$.” Note that $P(0)$ is true because $r_0 = s_0$ implies $r_0 = s_0$. Now assume for induction that $P(k)$ is true. In this case we want to prove that $P(k+1)$ is true.

So consider any $r_0, \ldots, r_{k+1}$ and $s_0, \ldots, s_{k+1}$ in the set $\{0, 1, \ldots, b-1\}$ and suppose that

$$r_0 + r_1 b + \cdots + r_{k+1} b^{k+1} = s_0 + s_1 b + \cdots + s_{k+1} b^{k+1}.$$

In this case we will prove that $r_i = s_i$ for all $i \in \{0, \ldots, k+1\}$. To do this we apply "division mod b" to both sides:

$$r_0 + b(r_1 + r_2 b \cdots + r_{k+1} b^k) = s_0 + b(s_1 + s_2 b \cdots + s_{k+1} b^k).$$

Since $r_0, s_0 \in \{0, 1, \ldots, b-1\}$ we know that these are the remainders and the bracketed expressions are the quotients. Thus by uniqueness of remainders we have $r_0 = s_0$ and by uniqueness of quotients we have

$$r_1 + r_2 b \cdots + r_{k+1} b^k = s_1 + s_2 b \cdots + s_{k+1} b^k.$$

But each of these expressions has coefficients in $\{0, 1, \ldots, b-1\}$ and highest power k. Since we have assumed that $P(k)$ is true, it follows that $r_i = s_i$ for all $i \in \{1, \ldots, k+1\}$.

In summary, we have shown that $r_i = s_i$ for all $i \in \{0, 1, \ldots, k+1\}$. □

[Remark: For any $b \geq 2$ we have proved that every non-negative integer has a unique "positional base b" representation. You are probability familiar with this result when $b = 10$. The modern positional base 10 system was developed in India around 500 AD and spread outward from there. It was fully adopted in Europe by the 15th century and it was fully adopted in East Asia by the 19th century.]