Math 561/661 **Exam 2**
Fall 2021 **Fri Nov 5**

Problem 1. Divisibility. Let $(R, +, \cdot, 0, 1)$ be a ring.

(a) Given elements $a, b \in R$, state the definition of the symbol "$a|b$".

$$a|b \iff \exists k \in R, ak = b$$

(b) If $a|b$ and $a|c$ for some $a, b, c \in R$, prove that $a|(bx + cy)$ for all $x, y \in R$.

Suppose that $a|b$ and $a|c$, so there exist elements $k, \ell \in R$ satisfying $ak = b$ and $b\ell = c$. It follows that $c = (ak)\ell = a(k\ell)$ and hence $a|c$.

(c) Given $a, b \in R$ we let $\text{Div}(a, b) = \{d \in R : d|a \text{ and } d|b\}$ denote the set of common divisors. If $a = bx + c$ for some $a, b, c, x \in R$, prove that $\text{Div}(a, b) = \text{Div}(b, c)$.

First suppose that $d \in \text{Div}(a, b)$, which means that $dk = a$ and $d\ell = b$ for some elements $k, \ell \in R$. Since $a = bx+c$ this implies that $c = a-bx = dkx-d\ell = d(kx-\ell)$ and hence $d|c$. Since we already have $d|b$ this implies that $d \in \text{Div}(b, c)$. Conversely, suppose that $d \in \text{Div}(b, c)$, which implies that $dk = b$ and $d\ell = c$ for some elements $k, \ell \in R$. Since $a = bx + c$ this implies that $a = bx + c = dkx + d\ell = d(kx + \ell)$ and hence $d|a$. Since we already have $d|b$ this implies that $d \in \text{Div}(a, b)$.

(d) Assume that R is an integral domain. If nonzero elements $a, b \in R$ satisfy $a|b$ and $b|a$, prove that $au = b$ for some element $u \in R$ satisfying $u|1$.

Suppose that nonzero elements $a, b \in R$ satisfy $a|b$ and $b|a$. This means that $ak = b$ and $b\ell = a$ for some elements $k, \ell \in R$, so that

$$\begin{aligned} a &= b\ell \\ a &= ak\ell \\ a(1 - k\ell) &= 0. \end{aligned}$$

Since $a \neq 0$ and since R is a domain, this implies that $1 - k\ell = 0$ and hence $k\ell = 1$. Taking $u = k$ gives $au = b$ for some element $u \in R$ satisfying $u|1$.

(e) Suppose that we have $ax + by = 1$ for some $a, b, x, y \in R$. If $a \neq 0$ and $a|(bc)$ for some $c \in R$, prove that we must have $a|c$.

Since $a|(bc)$ we can write $bc = ak$ for some element $k \in R$. Then we have

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

and hence $a|c$.

Problem 2. Modular Arithmetic. Fix an integer $n \geq 1$. Then for all integers $a, b \in \mathbb{Z}$ we say $a \equiv b \bmod n$ to mean that $n|(a-b)$.

(a) If $a \equiv b \bmod n$ and $b \equiv c \bmod n$, prove that $a \equiv c \bmod n$.

Suppose that $a \equiv b \bmod n$ and $b \equiv c \bmod n$, so that $a - b = nk$ and $b - c = n\ell$ for some integers $k, \ell \in \mathbb{Z}$. It follows that

$$a - c = (a-b) + (b-c) = nk + n\ell = n(k+\ell),$$

and hence $a \equiv c \bmod n$.

(b) If $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$, prove that $ab \equiv a'b' \bmod n$.

Suppose that $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$, so that $a - a' = nk$ and $b - b' = n\ell$ for some integers $k, \ell \in \mathbb{Z}$. It follows that

$$\begin{aligned} ab - a'b' &= ab - ab' + ab' - a'b' \\ &= a(b-b') + (a-a')b' \\ &= an\ell + nkb' \\ &= n(a\ell + kb'), \end{aligned}$$

and hence $ab \equiv a'b' \bmod n$.

(c) If $ab \equiv 1 \bmod n$ for some $a, b \in \mathbb{Z}$, prove that $\gcd(a, n) = 1$.

Suppose that $ab \equiv 1 \bmod n$, so that $ab - 1 = nk$ for some integer $k \in \mathbb{Z}$. In order to prove that $\gcd(a, n) = 1$ we will prove that the only common divisors of a and n are ± 1. So let d be any common divisor of a and n. This implies that $d\ell = a$ and $dm = n$ for some integers $\ell, m \in \mathbb{Z}$ and hence

$$1 = ab - nk = d\ell b - dmk = d(\ell b - mk).$$

Since $d|1$ we conclude that $d = \pm 1$ as desired.[1]

(d) Use the Vector Euclidean Algorithm to find some $x \in \mathbb{Z}$ satisfying $11x \equiv 1 \bmod 29$.

Consider the set of triples $(x, y, z) \in \mathbb{Z}^3$ such that $11x + 29y = z$. We perform $\mathbb{Z}$-linear combinations on the triples $(0, 1, 29)$ and $(1, 0, 11)$ until we reduce the third coordinate to 1:

x	y	z
0	1	29
1	0	11
-2	1	7
3	-1	4
-5	2	3
8	-3	1

It follows that $11(8) + 29(-3) = 1$ and hence $11 \cdot 8 \equiv 1 \bmod 29$.

[1]Short proof: $d|1$ implies $d \neq 0$ and $|d| \leq |1| = 1$.