Math 309 **Summer B 2018**
Homework 4 **Drew Armstrong**

---

1. Squares Mod 4. Every integer $n \in \mathbb{Z}$ has a unique "remainder mod 4." Let us use the notation $(n \bmod 4) \in \{0,1,2,3\}$ to denote this remainder.

(a) For all $x \in \mathbb{Z}$, show that $(x^2 \bmod 4) \in \{0,1\}$. [Hint: There are four kinds of integers. Square them all and see what you get.]

(b) Let $x, y, z \in \mathbb{Z}$ be integers satisfying the equation

$$x^2 + y^2 = z^2.$$

Prove that at least one of x, y must be even. [Hint: Assume for contradiction that x and y are both odd, which implies that x^2 and y^2 are both odd. Now use part (a) to get a contradiction.]

(a) Let $x \in \mathbb{Z}$ be any integer. By the Division Theorem, we know that the remainder $(x \bmod 4)$ is in the set $\{0,1,2,3\}$. In other words, we know that x has one of the following forms:

- If $(x \bmod 4) = 0$ then $x = 4k + 0$ for some $k \in \mathbb{Z}$.
- If $(x \bmod 4) = 1$ then $x = 4k + 1$ for some $k \in \mathbb{Z}$.
- If $(x \bmod 4) = 2$ then $x = 4k + 2$ for some $k \in \mathbb{Z}$.
- If $(x \bmod 4) = 3$ then $x = 4k + 3$ for some $k \in \mathbb{Z}$.

Let us square all four kinds of numbers and see what happens:

- If $(x \bmod 4) = 0$ then
$$x^2 = (4k+0)^2 = 16k^2 = 4(4k^2) + 0,$$
and hence $(x^2 \bmod 4) = 0$.
- If $(x \bmod 4) = 1$ then
$$x^2 = (4k+1)^2 = 16k^2 + 8k + 1 = 4(4k^2 + 2k) + 1,$$
and hence $(x^2 \bmod 4) = 1$.
- If $(x \bmod 4) = 2$ then
$$x^2 = (4k+2)^2 = 16k^2 + 16k + 4 = 4(4k^2 + 4k + 1) + 0,$$
and hence $(x^2 \bmod 4) = 0$.
- If $(x \bmod 4) = 3$ then
$$x^2 = (4k+3)^2 = 16k^2 + 24k + 9 = 4(4k^2 + 12k + 2) + 1,$$
and hence $(x^2 \bmod 4) = 1$.

In any case, we find that $(x^2 \bmod 4) \in \{0,1\}$. More precisely, we can say that

$$\begin{aligned}(x \text{ is even}) &\Leftrightarrow (x^2 \bmod 4) = 0,\\ (x \text{ is odd}) &\Leftrightarrow (x^2 \bmod 4) = 1.\end{aligned}$$

(b) *Proof:* Suppose that integers $x, y, z \in \mathbb{Z}$ satisfy the equation

$$x^2 + y^2 = z^2,$$

and let us **assume for contradiction** that both x and y are odd. From part (a) this implies that $(x^2 \bmod 4) = 1$ and $(y^2 \bmod 4) = 1$, hence there exist integers $k, \ell \in \mathbb{Z}$ such that

$$x^2 = 4k + 1 \qquad \text{and} \qquad y^2 = 4\ell + 1.$$

But then the equation

$$z^2 = x^2 + y^2 = (4k+1) + (4\ell+1) = 4(k+\ell) + 2$$

implies that $(z^2 \bmod 4) = 2$, which is a contradiction to part (a). $\square$

2. Euclidean Algorithm.

(a) Apply the Euclidean Algorithm to compute the greatest common divisor of 62 and 24.

(b) Apply the Extended Euclidean Algorithm to find all **integer** solutions $x, y \in \mathbb{Z}$ to the linear equation

$$62x + 24y = 4.$$

Hint: You need to find the complete solution of the "homogeneous" equation

$$62x_0 + 24y_0 = 0,$$

and one particular solution of the "non-homogeneous" equation

$$62x' + 24y' = 4.$$

Then the complete solution is $x = x_0 + x'$ and $y = y_0 + y'$.

I will do parts (a) and (b) at the same time. Let us consider the set of triples $(x, y, z) \in \mathbb{Z}^3$ that satisfy the equation $62x + 24y = z$. We begin with the basic triples $(1, 0, 62)$ and $(0, 1, 24)$ and then apply the Euclidean Algorithm:

x	y	z	
1	0	62	(Row 1)
0	1	24	(Row 2)
1	-2	14	(Row 3) = (Row 1) $-$ 2 $\cdot$ (Row 2)
-1	3	10	(Row 4) = (Row 2) $-$ 1 $\cdot$ (Row 3)
2	-4	4	(Row 5) = (Row 3) $-$ 1 $\cdot$ (Row 4)
-5	13	$\boxed{2}$	(Row 6) = (Row 4) $-$ 2 $\cdot$ (Row 5)
12	-31	0	(Row 7) = (Row 5) $-$ 2 $\cdot$ (Row 6)

The smallest non-zero remainder is the greatest common divisor:

$$\gcd(62, 24) = 2.$$

Since the gcd divides 4, we can multiply Row 6 by 2 to obtain a particular solution $(x', y') = (-10, 26)$:

$$\begin{aligned} 62(-5) + 42(13) &= 2 \\ 62(-5 \cdot 2) + 42(13 \cdot 2) &= 2 \cdot 2 \\ 62(-10) + 42(26) &= 4. \end{aligned}$$

And multiplying Row 7 by an arbitrary integer $k \in \mathbb{Z}$ gives the homogeneous solution $(x_0, y_0) = (12k, -13k)$:

$$\begin{aligned} 62(12) + 42(-31) &= 0 \\ 62(12 \cdot k) + 42(-31 \cdot k) &= 0 \cdot k \\ 62(12k) + 42(-31k) &= 0. \end{aligned}$$

Adding these gives the complete solution:

$$\begin{array}{rrcl} & 62(-10)+42(26) & = & 4 \\ + & 62(12k)+42(-31k) & = & 0 \\ \hline & 62(-10+12k)+42(26-31k) & = & 4. \end{array}$$

In other words, the complete solution is

$$(x,y)=(x'+x_0,y'+y_0)=(-10+12k,26-13k) \quad \text{for any } k\in\mathbb{Z}.$$

3. Divisibility. For all integers $a,b\in\mathbb{Z}$ we define the divisibility relation as follows:

$$\text{“}a \text{ divides } b\text{”} = \text{“}a|b\text{”} = \text{“}\exists k\in\mathbb{Z}, ak=b.\text{”}$$

Let $a,b,c\in\mathbb{Z}$ and prove the following properties of divisibility.

(a) If $a|b$ and $b|c$ then $a|c$.
(b) If $a|b$ and $a|c$ then $a|(bx+cy)$ for all $x,y\in\mathbb{Z}$.
(c) If $a|b$ and $b|a$ then $a=\pm b$.

(a) If $a|b$ and $b|c$ then there exist integers $k,\ell\in\mathbb{Z}$ with

$$b=ak \qquad \text{and} \qquad c=b\ell.$$

But then we have

$$c=b\ell=(ak)\ell=a(k\ell),$$

which implies that $a|c$.

(b) If $a|b$ and $a|c$ then there exist integers $k,\ell\in\mathbb{Z}$ with

$$b=ak \qquad \text{and} \qquad c=a\ell.$$

Then for any integers $x,y\in\mathbb{Z}$ we have

$$bx+cy=(ak)x+(a\ell)y=a(kx+\ell y),$$

which implies that $a|(bx+cy)$.

(c) First let me repeat an observation from class:

$$\text{If } a|b \text{ and } b\neq 0 \text{ then } |a|\leq|b|.$$

To see this, suppose that $a|b$ and $b\neq 0$. Since $a|b$ we have $b=ak$ for some $k\in\mathbb{Z}$ and then since $b\neq 0$ we also have $k\neq 0$. But then since k is a whole number and since $|a|$ is positive we have

$$\begin{aligned} 1&\leq|k| \\ |a|&\leq|a|\cdot|k| \\ |a|&\leq|a\cdot k| \\ |a|&\leq|b|. \end{aligned}$$

Now we solve part (c). Let $a|b$ and $b|a$ so that $a=bk$ and $b=a\ell$ for some integers $k,\ell\in\mathbb{Z}$. If $a=0$ then $b=a\ell=0\ell=0$ and if $b=0$ then $a=bk=0k=0$. In either case the equation $a=\pm b$ is true. Otherwise, let us assume that $a\neq 0$ and $b\neq 0$. Then

$$a|b \text{ and } b\neq 0 \text{ implies } |a|\leq|b|$$

and

$$b|a \text{ and } a\neq 0 \text{ implies } |b|\leq|a|.$$

We conclude that

$$|a| = |b|$$

as desired.

4. Euclid's Lemma. Let $a, b, c \in \mathbb{Z}$ and prove the following:

$$\text{if } a|bc \text{ and } \gcd(a, b) = 1 \text{ then } a|c.$$

Hint: If $\gcd(a, b) = 1$ then one may use the Extended Euclidean Algorithm to find some integers $x, y \in \mathbb{Z}$ satisfying

$$ax + by = 1.$$

Multiply both sides of this equation by c and see what happens.

Proof: Consider integers $a, b, c \in \mathbb{Z}$ with $a|(bc)$ and $\gcd(a, b) = 1$. Since $a|(bc)$ there exists an integer $k \in \mathbb{Z}$ such that

$$bc = ak,$$

and since $\gcd(a, b) = 1$ there exist integers $x, y \in \mathbb{Z}$ (from the Euclidean Algorithm) such that

$$ax + by = 1.$$

Then multiplying both sides by c gives

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

and hence $a|c$.

Remark. You might see Euclid's Lemma stated in a slightly different form. Consider integers $a, b, p \in \mathbb{Z}$ where p is **prime**. Then the following is true:

$$\text{If } p|(ab) \text{ then } p|a \text{ or } p|b.$$

After a bit of work, this result leads to the theorem that every integer has a "unique prime factorization."