Assignment 1 – All 2 parts – Math 412

Due in class: Thursday, Sept. 5, 2019

Textbook exercises:
Section 1.1: 6 (WI), 8 (WI)
Section 1.2: 6, 8, 11, 16, 30

1 1.1.6

Since the quotient of q divided by c is k, we can express this in the form $q = ck+\alpha, 0 \leq \alpha < c$. Notice now that $a = bq+r$ can be rewritten as $a = b(ck+\alpha)+r = bck+b\alpha+r = (bc)k+(b\alpha+r)$. Now if $b\alpha + r < bc$, we have the desired form and it is clear to see that bc divides a with quotient k. If $b\alpha+r \geq bc$, since $b\alpha+r \in \mathbb{Z}$, we can rewrite $b\alpha+r = \beta bc+s$, with $0 \leq s < bc$. Then we have that $a = (bc)k + (b\alpha + r) = (bc)(k + \beta) + s$. Again we find that bc divides a with quotient k.

2 1.1.8

Suppose $\alpha \in \mathbb{Z}$. We have that α must be either odd or even. By using the Division Algorithm, we know that for $\alpha \in \mathbb{Z}$, we should be able to express any α in the form $\alpha = 2k$ or $\alpha = 2k+1$. Suppose α is odd. Then $\alpha = 2k + 1, k \in \mathbb{Z}$. Moreover, $2\alpha = 4k + 2$, with 2α even. It follows that $2\alpha + 1 = 4k + 3$ is odd.
Suppose α is even. Then $\alpha = 2k, k \in \mathbb{Z}$. Moreover, $2\alpha = 4k$, and we have that $2\alpha+1 = 4k+1$. Again by using the Division Algorithm, we let α range over all $\mathbb{Z}$. We can construct any odd integer and find that $2\alpha + 1 = 4k + 1$ or $2\alpha + 1 = 4k + 3$, as required.

3 1.2.6

If $a \mid b$, and $c \mid d$, there exist $k, j \in \mathbb{Z}$ such that $ka = b$ and $jc = d$. By multiplying these two equations together we get that $bd = kajc = (ac)kj$. $kj \in \mathbb{Z}$, so we can also say that $ac \mid bd$.

4 1.2.8

Let us name the common divisors of n and $n + 1$ as α. We can then say that there exist $j, k \in \mathbb{Z}$ such that $\alpha k = n, \alpha j = n+1$. By subtracting, we get that $\alpha j-\alpha k = \alpha(j-k) = 1$ The

two factors $(j-k)$ and α must be integers, so the only ways to obtain 1 are if $\alpha = j-k = \pm 1$. It follows that $(n, n+1) = 1$.

5 1.2.11

I will apply a similar approach to the above problem, taking α to be an arbitrary common divisor.

5.1 a

By assuming a common divisor, we have $j, k \in \mathbb{Z}$ such that $n = j\alpha, n+2 = k\alpha$. Then we have that $\alpha(k-j) = 2$. Since these factors are integers and we only want to worry about the greatest divisor, let us ignore negative factors. In this case we have that $\alpha(k-j) = 2*1$ or $\alpha(k-j) = 1*2$. It follows that $(n, n+2) = 1$ or $(n, n+2) = 2$.

5.2 b

Using a similar construction to part a, we get that $6 = \alpha(k-j)$. The possible ways to make 6 from positive integers are $1*6, 2*3, 3*2, 6*1$. It follows that $(n, n+6) \in \{1, 2, 3, 6\}$.

6 1.2.16 ???

If $(a, b) = d$, then d divides both a and b. We can take $r, s \in \mathbb{Z}$ such that $a = ds, b = dr$. Moreover, $a/d = s, b/d = r$. By Theorem 1.2 we can say that $d = au + bv$ and $1 = \frac{a}{d}u + \frac{b}{d}v = su + rv$.

7 1.2.30

The first step would be to prove that the set $S = \{a_1u_1 + ... + a_nu_n | u_i \in \mathbb{Z}\}$ is nonempty. We take the sum $a_1^2 + ... + a_n^2 \geq 0$ since not all a_i can be 0 to prove that S has an element. It follows that we may use the Well-Ordering Axiom to get the smallest positive element of S, call it $t = a_1u_1 + ... + a_nu_n, a_i \in \mathbb{Z}$.
We may assume a_i to be any of the integers contained in the sum. By the Division Algorithm, we have that there exist $q_i, r_i \in \mathbb{Z}$ such that $a_i = tq_i + r_i, 0 \leq r_i < t$. It follows that $r_i = a_i - tq_i = a_i - (a_1u_1 + ... + a_nu_n)q_i = a_i(1 - q_iu_i) + a_1(-u_iq_i) + ... + a_{i-1}(-u_{i-1}q_i) + a_{i+1}(-u_{i+1}q_i) + ... + a_n(-u_nq_i)$. This is a linear combination of a_i's, and by using the

assumption that t is the smallest positive element we can conclude that $r = 0$. It follows that $t|a_i$.

Let c be another common divisor of a_i's. Then for some $k_i \in \mathbb{Z}$, we have $a_i = ck_i$. It follows that $t = a_1u_1 + ... + a_nu_n = (ck_1)u_1 + ... + (ck_n)u_n = c(k_1u_1 + ... + k_nu_n)$. So $c|t$, and $c \leq \|t\|$ but t is positive so $c \leq t$.

Thus t satisfies the conditions for being the gcd d.

Other exercises:

(1) Sums of three squares. In class, we showed that if n has remainder 3 when divided by 4, then n cannot be written as a sum of two squares. This question gives a similar result for sums of three squares.

(a) Show that when divided by 8, the square of any integer has remainder either $0, 1$, or 4.

We can represent any integer, n, by the form $n = 8k + r$, with $k \in \mathbb{Z}, r \in \{0, 1, 2, 3, 4, 5, 6, 7\}$. Now I can compute.

(i) $(8k + 0)^2 = 64k^2 = 8(8k^2) + 0$.

(ii) $(8k + 1)^2 = 64k^2 + 16k + 1 = 8(8k^2 + 2k) + 1$.

(iii) $(8k + 2)^2 = 64k^2 + 32k + 4 = 8(8k^2 + 4k) + 4$.

(iv) $(8k + 3)^2 = 64k^2 + 48k + 9 = 8(8k^2 + 6k + 1) + 1$.

(v) $(8k + 4)^2 = 64k^2 + 64k + 16 = 8(8k^2 + 8k + 2) + 0$.

(vi) $(8k + 5)^2 = 64k^2 + 80k + 25 = 8(8k^2 + 10k + 3) + 1$.

(vii) $(8k + 6)^2 = 64k^2 + 96k + 36 = 8(8k^2 + 12k + 4) + 4$.

(viii) $(8k + 7)^2 = 64k^2 + 112k + 49 = 8(8k^2 + 14k + 6) + 1$.

In all cases we have something of the form $8k + r$, where $r \in \{0, 1, 4\}$.

(b) Conclude that if n has remainder 7 when divided by 8, then n cannot be written as a sum of three squares.

In class we used the fact that the sum of remainders (modulo 8) is the remainder of the sum. The above argument also proved that any number squared then divided by 8 must have a remainder of $0, 1, 4$. It is impossible to create a sum of 7 from three numbers of the set $\{0, 1, 4\}$. Thus, it is impossible for any number that is the sum of three squares to have a remainder of 7 when divided by 8.

(c) Give an example of a number of the form $4k+3$, $k \in \mathbf{Z}$, that *is* a sum of three squares.

A very simple example is

$$1^2 + 1^2 + 1^2 = 1 + 1 + 1 = 3 = 4 * 0 + 3. \tag{1}$$

(2) (WI) Let a and b be positive integers, and let $g = (a, b)$. Suppose $u_0, v_0 \in \mathbf{Z}$ are such that $g = au_0 + bv_0$.

(a) Let $k \in \mathbf{Z}$ and let

$$u = u_0 + \frac{bk}{g} \quad \text{and} \quad v = v_0 - \frac{ak}{g}.$$

Show that $au + bv = g$.

From the assumptions we get that $u_0 = u - \frac{bk}{g}, v_0 = v + \frac{ak}{g}$. So $au_0 = au - \frac{bka}{g}, bv_0 = bv + \frac{bak}{g}$, and by adding these two equations we can see that $g = au + bv$ as required.

(b) Conversely, show that if $g = au + bv$ with $u, v \in \mathbf{Z}$, then there is an integer k such that

$$u = u_0 + \frac{bk}{g} \quad \text{and} \quad v = v_0 - \frac{ak}{g}.$$