MAT 312/AMS 351: Applied Algebra
Solutions to Problem Set 2 (18pts)

1.4 5; 3pts *Show that no integer of the form $8n+7$ is a sum of three squares (of integers).*

Suppose $n, a, b, c \in \mathbb{Z}$ are such that $a^2+b^2+c^2=8n+7$ and so

$$a^2+b^2+c^2 \equiv 7 \mod 8.$$

Since $a, b, c \equiv 0, \pm 1, \pm 2, \pm 3, 4 \mod 8$,

$$a^2, b^2, c^2 \equiv 0, 1, 4, 9, 16 \equiv 0, 1, 4, 1, 0 \mod 8 \quad \Longrightarrow \quad a^2+b^2+c^2 \equiv 0, 1, 2, 3, 4, 5, 6 \mod 8.$$

This contradicts the first equation, and so no integer of the form $8n+7$ is a sum of three squares.

1.4 6; 3pts *Let p be a prime number. Show that the equation $x^2=[1]_p$ has just two solutions in $\mathbb{Z}_p$.*

Suppose $a \in \mathbb{Z}$ and $a^2 \equiv 1 \mod p$. Thus, p divides

$$a^2-1 = (a-1)(a+1).$$

Since p is prime, it follows that p divides either $a-1$ (in which case $[a]_p=[1]_p$) or $a+1$ (in which case $[a]_p=-[1]_p$). Thus, the only possible solutions of $x^2=[1]_p$ in $\mathbb{Z}_p$ are $x=\pm[1]_p$ and these are indeed solutions. If $p>2$, $[1]_p \neq -[1]_p$ and so these two solutions are distinct. If $p=2$, $[1]_p=-[1]_p$ and so these two solutions are the same.

1.4 7; 3pts *Let p be a prime number. Show that $(p-1)! \equiv -1$ mod p.*

If $p=2$, this just says that $1 \equiv -1 \mod 2$. So, we assume that $p>2$. Every number i appearing in the product

$$(p-1)! \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1)$$

is relatively prime to p and thus has an inverse i_p^{-1} mod p by Theorem 1.4.3, which also appears somewhere in this product. By 1.4 6, this inverse i_p^{-1} is different from i unless $i=1$ or $i=p-1$ (in which case $i \equiv -1 \mod p$). We can thus multiply every factor i appearing in $(p-1)!$, other than 1 and $p-1$, with its inverse i_p^{-1} mod p and throw the two out of the product (because $i \cdot i_p^{-1} \equiv 1$ mod p). We are then left only with $1 \cdot (p-1)$, which is congruent to -1 mod p. This establishes the claim.

1.5 3; 4pts *Find the smallest positive integer whose remainder when divided by 11 is 8, which has the last digit 4, and is divisible by 27.*

We need to solve the system

$$\begin{cases} x \equiv 8 \mod 11 \\ x \equiv 4 \mod 10 \\ x \equiv 0 \mod 27 \end{cases}$$

The first equation means that $x=8+11k$ for some $k\in\mathbb{Z}$. So, we need to find k such that

$$8+11k \equiv 4 \bmod 10, \qquad k \equiv -4.$$

By the Chinese Remainder Theorem, the unique mod $11\cdot10$ solution of the first two equations above is thus

$$x \equiv 8+11(-4) = -36 \mod 110.$$

In order to satisfy the third equation, we then need to find $m\in\mathbb{Z}$ so that

$$-36+110m \equiv 0 \bmod 27, \qquad 2m \equiv 9 \bmod 27.$$

Since $14\cdot2\equiv1 \bmod 27$, multiplying the last equation by 14 gives

$$m \equiv 14\cdot9 \equiv 18 \mod 27, \qquad x \equiv -36+110\cdot18 = 1944 \mod 110\cdot29.$$

By the Chinese Remainder Theorem, the smallest positive integer that works is thus $\boxed{1944}$

Alternatively, $1\cdot11-1\cdot10=1$. As stated in the book, this implies that

$$1\cdot11\cdot4-1\cdot10\cdot8 = -36$$

is the mod 110 solution of the first pair of equations. Euclid's algorithm gives

$$\begin{aligned} &(1):\ \mathbf{110} = 4\cdot\mathbf{27}+\mathbf{2} && \gcd(\mathbf{27},\mathbf{110}) = \mathbf{1} \overset{(2)}{=\!=} \mathbf{27} - 13\cdot\mathbf{2} \\ &(2):\ \mathbf{27} = 13\cdot\mathbf{2}+\mathbf{1} && \overset{(1)}{=\!=} \mathbf{27} - 13\cdot(\mathbf{110}-4\cdot\mathbf{27}) = 53\cdot\mathbf{27}-13\cdot\mathbf{110}. \\ &(3):\ \mathbf{2} = 2\cdot\mathbf{1}+0 && \end{aligned}$$

Thus, $53\cdot27-13\cdot110=1$. As stated in the book, this implies that

$$53\cdot27\cdot(-36)-13\cdot110\cdot0 = -51516 \equiv 1944 \mod 110\cdot29.$$

The smallest positive integer that works is thus $\boxed{1944}$

Problem A (2+3pts)

A museum has a collection of blue, green, and red chameleons. When two chameleons of different colors meet, they both turn into the third color (if a blue and green meet, for example, they both turn red). The collection initially contains B blue, G green, and R red chameleons (B, G, R are nonnegative integers).

(a) *Suppose all chameleons eventually turn the same color. Show that*

$$(B-G)(G-R)(R-B) = 0 \mod 3.$$

(b) *Suppose the above condition holds. Show that there exists a sequence of meetings so that all chameleons eventually turn the same color.*

(a) When two chameleons of different colors meet (say, blue and green), their numbers go down by 1 (say, B and G become $B-1$ and $G-1$) and the number of the third color goes up by 2 (say, R becomes $R+2$). Thus, the three differences $B-G$, $G-R$, and $R-B$ change by a multiple of 3 (3 times 0 or ± 1), i.e. they are *constant mod 3* and so is their product. If all chameleons eventually turn the same color, two of the numbers B, G, R become 0 and thus the product above becomes 0. Since it is constant mod 3, it was 0 mod 3 to begin with.

(b) If the product of $B-G$, $G-R$, and $R-B$ is divisible by 3, then 3 divides one of these factors (because 3 is prime). By symmetry, we can assume that $B-G=3k$ for some $k \in \mathbb{Z}^{\geq 0}$ (in particular, $B \geq G$). If $G \neq 0$, we can have each of the greens meet one of the blues so that all of the greens disappear. Thus, we can assume that $G = 0$ and $B = 3k$ for some $k \in \mathbb{Z}^{\geq 0}$. If $R = 0$, then all chameleons are already of one color (blue) and there is nothing to prove. Otherwise, we show by induction on k that there exists a sequence of meetings so that all chameleons eventually turn red. There is nothing to prove in the base $k = 0$ case (when all chameleons are red to begin with). Suppose such a sequence exists whenever $B=3k$ for some $k \in \mathbb{Z}^{\geq 0}$, $G=0$, and $R>0$. We show that this is also the case if $B=3(k+1)$, $G=0$, and $R>0$. In this case, we first have a blue and a red chameleon meet to reduce B and R by 1 and make $G=2$; since $k \geq 0$, there are still at least 2 blues. We then have 2 of the blues and the 2 greens meet to produce 4 reds, thus taking the number of blues to $B=3k$, the number of greens back to $G=0$, and the number of reds to $-1+4=3$ higher than what we had started with. By the inductive assumption, there exists a sequence of meetings so that all chameleons eventually turn red from this new situation and thus there exists such a sequence from the initial one (since we are able to get to this new situation from the original one). By induction, this implies that such a sequence exists for all k.

Alternative Proof. Let

$$S = \Big\{ \min\big\{\{|B-G|, |G-R|, |R-B|\}\cap 3\mathbb{Z}^{\ge 0}\big\} : \text{achievable } (B,G,R)\Big\}.$$

By the proof of (a) and the first sentence in the first proof of (b), at least one of $|B-G|$, $|G-R|$, and $|R-B|$ is divisible by 3 (i.e. lies in $3\mathbb{Z}$) and so

$$\min\big\{\{|B-G|, |G-R|, |R-B|\}\cap 3\mathbb{Z}^{\ge 0}\big\} \in 3\mathbb{Z}^{\ge 0} \subset \mathbb{Z}^{\ge 0}$$

is a well-defined nonnegative integer for every combination (B,G,R) achievable from the given starting triple. Thus, S is a nonempty subset of $\mathbb{Z}^{\ge 0}$. By the Well-Ordering Principle, S then contains a minimal element $s_0 \in 3\mathbb{Z}^{\ge 0}$. If $s_0 = 0$, then two of the three numbers, say B and G, are the same. The blue and green chameleons can then meet and turn into reds, leaving only one color.

Suppose $s_0 > 0$ (and thus $s_0 \ge 3$) and is achieved by $s_0 = B-G$ for some triple (B,G,R). Since $s_0 > 0$, either $G > 0$ or $R > 0$ (or both). If $R > 0$, a blue and a red can meet turning into 2 greens. This decreases B by 1, increases G by 2, and thus decreases $|G-R| = s_0 \in 3\mathbb{Z}^+$ by 3. However, this contradicts the assumption that $s_0 \in S$ is the minimal possible value for all achievable triples (B,G,R). If $G > 0$ (and thus $B = G+s_0 \ge 4$), a blue and a green can meet turning into 2 reds. After that, another blue can meet with a red turning into 2 blues. These two meetings decrease B by 2, increase G by $-1+2$, and thus decrease $|G-R| = s_0 \in 3\mathbb{Z}^+$ by 3. This again contradicts the assumption that $s_0 \in S$ is the minimal. We conclude that $s_0 = 0$ and so the conclusion of the last sentence of the previous paragraph applies.