Math 400 — Take Home Exam
Due: Friday, March 19

Dana Merrick
June 14, 2010

(1) (a) Consider the quantity x represented in base ten fractional from by $\frac{7}{9}$.

(i) Represent x as a *finite* sum of *distinct* unit fractions.

Solution. $\frac{1}{2} + \frac{1}{4} + \frac{1}{36}$

(ii) Represent x in base 3 form.

Solution. $(0.21)_3$

(iii) Represent x in base 8 form.

Solution. $(0.\overline{61})_8$

(iv) Represent x in base 16 form.

Solution. $(0.\overline{\text{C71}})_{16}$

(b) Prove that every positive integer can be *uniquely* represented as the sum or difference of powers of 3 (e.g. $11 = 3^3 - 3^2 - 3^1 - 3^0$).
Hint: Consider the base 3 representation of integers and induct on p, the *number* of symbols in the base 3 representation.

Proof. Assume that every positive integer n can be uniquely represented as the sum or difference of powers of 3. We will proceed by induction on p, the number of symbols in the base 3 representation of n.
Notice that any time we're given 2 as a coefficient in the sum/difference of powers of 3 representation, we can rewrite it as $2 = 3 - 1$. Therefore, for any $i \in \mathbb{Z}$ we have that:

$$2 \cdot 3^i = 3 \cdot 3^i - 1 \cdot 3^i = 3^{i+1} - 3^i.$$

This allows us to "shift left" the base 3 representation of n.
As a base case, the proposition is true because when $p = 1$, we find that $1 = 3^0$. Next, assume that the proposition is true for $p = k$. We want to show that the supposition is true for $p = k + 1$.
In other words, $p = k + 1$ implies we are adding another position to the base 3 representation. We really only care if the new position contains a 2. If the k+1th position is occupied by a 2, then $2 \cdot 3^{k+1}$ is in the base 3 representation. However, since $2 \cdot 3^{k+1} = 3^{k+2} - 3^{k+2}$, we can convert any 2 we find such that every digit in the base 3 representation is either 0 or ± 1.

Hence, every n can be uniquely represented as the sum or difference of powers of 3. $\square$

(2) The algebraic structure $(\mathbb{Z}_3, +, \cdot)$ is the set $\{0, 1, 2\}$ together with the operations of arithmetic (addition and multiplication) modulo 3. This structure is an example of a (finite) field. The vector space $V = (\mathbb{Z}_3)^3$ is a vector space over the field $\mathbb{Z}_3$. V has $3^3 = 27$ vectors, 26 of which are nonzero. The dimension of V is 3, and all of the results associated with vector spaces apply.

There are 26 letters in our alphabet, and we may correspond each letter to a nonzero vector in V according to the letter's position. Thus,

$$A \leftrightarrow \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

and

$$Z \leftrightarrow \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix}$$

The usual basis $B = \{\epsilon_1, \epsilon_2, \epsilon_3\}$ corresponds to letters I, C, and A respectively.

(a) Consider the mapping $\varphi : (\mathbb{Z}_3)^3 \to (\mathbb{Z}_3)^3$ given by:

$$\varphi\left(\langle a_1, a_2, a_3\rangle\right) = \langle a_1 + a_2, a_2 + a_3, a_1 + a_3\rangle$$

(i) Show φ is *linear.*

Proof. Recall that φ is linear if for any two vectors α, $\beta \in (\mathbb{Z}_3)^3$ and a constant c, the following two conditions are satisfied:

$$\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$$

and

$$\varphi(c \cdot \alpha) = c \cdot \varphi(\alpha).$$

Let $\alpha = \langle a_1, a_2, a_3\rangle$ and $\beta = \langle b_1, b_2, b_3\rangle$. Then we have the following:

$$\begin{aligned}
\varphi(\alpha) + \varphi(\beta) &= \langle a_1 + a_2, a_2 + a_3, a_1 + a_3\rangle + \langle b_1 + b_2, b_2 + b_3, b_1 + b_3\rangle \\
&= \langle a_1 + b_1 + a_2 + b_2, a_2 + b_2 + a_3 + b_3, a_1 + b_1 + a_3 + b_3\rangle \\
&= \varphi(\langle a_1 + b_1\rangle, \langle a_2 + b_2\rangle, \langle a_3 + b_3\rangle) \\
&= \varphi(\alpha + \beta)
\end{aligned}$$

and

$$
\begin{aligned}
c \cdot \varphi(\alpha) &= c \cdot \langle a_1 + a_2, a_2 + a_3, a_1 + a_3 \rangle \\
&= \langle c \cdot (a_1 + a_2), c \cdot (a_2 + a_3), c \cdot (a_1 + a_3) \rangle \\
&= \varphi(c \cdot \alpha).
\end{aligned}
$$

Therefore, φ is linear. $\square$

(ii) Express φ in *matrix* form $A = (a_{ij})$.

Solution.

$$
A \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 \\ a_2 + a_3 \\ a_1 + a_3 \end{pmatrix}
$$

$$
A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}
$$

(iii) Compute $\det(A)$.

Solution.

$$
\det(A) = 1 + 1 + 0 - 0 - 0 - 0 = 1 + 1 = 2
$$

(iv) Explain why φ is *nonsingular*.

Solution. Recall that a matrix is nonsingular if and only if its determinate is nonzero. Since $\det(A) = 2$, φ is nonsingular.

(v) Since A is nonsingular, it is *invertible*. Determine A^{-1}.

Solution.

$$
\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} A^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
$$

$$
A^{-1} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}
$$

(b) With respect to the usual basis and the *natural* correspondence α between letters and V, determine:

$$
\lambda(\text{MATHEMATICS}), \text{ where}
$$

$$
\lambda = \alpha^{-1} \circ \varphi \circ \alpha
$$

(i) Give the *permutation* of letters associated with λ.

Solution. λ(MATHEMATICS) = ZDYWKZDYJLU

(c) Consider the *permutation* Π of letters that *reverses* letters, zyx...a.

(i) What is the *order* of Π?

Solution. The order of Π is 2, since $\Pi(\Pi(\gamma)) = \gamma$ for every γ.

(ii) Is the mapping

$$\alpha \circ \Pi \cdot \circ^{-1} : (\mathbb{Z}_3)^3 \to (\mathbb{Z}_3)^3$$

one-to-one? Justify your answer.

Solution. Yes. We know that α is one-to-one, which in turn implies that α^{-1} is one-to-one. Since Π is a permutation, Π is also one-to-one. Finally, the composition of one-to-one functions is always one-to-one.

(iii) Give the image of each nonzero vector in $(\mathbb{Z}_3)^3$ under $\alpha \circ \Pi \circ \alpha^{-1}$.

Solution.

$$\alpha \circ \Pi \circ \alpha^{-1}(A) = Z$$
$$\alpha \circ \Pi \circ \alpha^{-1}(B) = Y$$
$$\alpha \circ \Pi \circ \alpha^{-1}(C) = X$$
$$\alpha \circ \Pi \circ \alpha^{-1}(D) = W$$
$$\alpha \circ \Pi \circ \alpha^{-1}(E) = V$$
$$\alpha \circ \Pi \circ \alpha^{-1}(F) = U$$
$$\alpha \circ \Pi \circ \alpha^{-1}(G) = T$$
$$\alpha \circ \Pi \circ \alpha^{-1}(H) = S$$
$$\alpha \circ \Pi \circ \alpha^{-1}(I) = R$$
$$\alpha \circ \Pi \circ \alpha^{-1}(J) = Q$$
$$\alpha \circ \Pi \circ \alpha^{-1}(K) = P$$
$$\alpha \circ \Pi \circ \alpha^{-1}(L) = O$$
$$\alpha \circ \Pi \circ \alpha^{-1}(M) = N$$

$$\alpha \circ \Pi \circ \alpha^{-1}(N) = M$$
$$\alpha \circ \Pi \circ \alpha^{-1}(O) = L$$
$$\alpha \circ \Pi \circ \alpha^{-1}(P) = K$$
$$\alpha \circ \Pi \circ \alpha^{-1}(Q) = J$$
$$\alpha \circ \Pi \circ \alpha^{-1}(R) = I$$
$$\alpha \circ \Pi \circ \alpha^{-1}(S) = H$$
$$\alpha \circ \Pi \circ \alpha^{-1}(T) = G$$
$$\alpha \circ \Pi \circ \alpha^{-1}(U) = F$$
$$\alpha \circ \Pi \circ \alpha^{-1}(V) = E$$
$$\alpha \circ \Pi \circ \alpha^{-1}(W) = D$$
$$\alpha \circ \Pi \circ \alpha^{-1}(X) = C$$
$$\alpha \circ \Pi \circ \alpha^{-1}(Y) = B$$
$$\alpha \circ \Pi \circ \alpha^{-1}(Z) = A$$

(d) Is $\alpha \circ \Pi \circ \alpha^{-1}$ *linear*? Justify your answer.

Note: Assume $\alpha \circ \Pi \circ \alpha^{-1} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

Solution. No. In order for $\alpha \circ \Pi \circ \alpha^{-1}$ to be linear, for any γ, $\delta \in (\mathbb{Z}_3)^3$ it must be true that:

$$\alpha \circ \Pi \circ \alpha^{-1}(\gamma + \delta) = \alpha \circ \Pi \circ \alpha^{-1}(\gamma) + \alpha \circ \Pi \circ \alpha^{-1}(\delta).$$

Consider the following:

$$\begin{aligned} \alpha \circ \Pi \circ \alpha^{-1}(A + A) &= \alpha \circ \Pi \circ \alpha^{-1}(\langle 001 \rangle + \langle 001 \rangle) \\ &= \alpha \circ \Pi \circ \alpha^{-1}(\langle 002 \rangle) \\ &= \alpha \circ \Pi \circ \alpha^{-1}(B) \\ &= Y \\ &= \langle 221 \rangle \end{aligned}$$

Additionally,

$$\begin{aligned}\alpha \circ \Pi \circ \alpha^{-1}(A) + \alpha \circ \Pi \circ \alpha^{-1}(A) &= Z + Z \\ &= \langle 222 \rangle + \langle 222 \rangle \\ &= \langle 111 \rangle \\ &= M\end{aligned}$$

Hence, $\alpha \circ \Pi \circ \alpha^{-1}(A + A) \neq \alpha \circ \Pi \circ \alpha^{-1}(A) + \alpha \circ \Pi \circ \alpha^{-1}(A)$.

(3) Let T_i denote the ith triangular number, $i \geq 1$.

(a) Derive formulas for the following:

(i) $\sum_{i=1}^{n} T_i$

Solution.

$$\begin{aligned}\sum_{i=1}^{n} T_i &= \sum_{i=1}^{n} \frac{i \cdot (i+1)}{2} \\ &= \frac{1}{6} n(n+1)(n+2)\end{aligned}$$

(ii) $\sum_{i=1}^{n} T_{2i-1}$

Solution.

$$\begin{aligned}\sum_{i=1}^{n} T_{2i-1} &= \sum_{i=1}^{n} \frac{i \cdot (4i-2)}{2} \\ &= \frac{1}{6} n(n+1)(4n-1)\end{aligned}$$

(iii) $\sum_{i=1}^{2n} (-1)^i T_i$

Solution.

$$\begin{aligned}\sum_{i=1}^{2n} (-1)^i T_i &= \sum_{i=1}^{n} (-1)^i \cdot \frac{i \cdot (i+1)}{2} \\ &= \frac{1}{8} (-1)^n \cdot [2n(n+2)+1] - 1\end{aligned}$$

(iv) $\sum_{i=1}^{n} (T_i)^2$

Solution.

$$\sum_{i=1}^{n}(T_i)^2 = \sum_{i=1}^{n}\left(\frac{i\cdot(i+1)}{2}\right)^2$$
$$= \frac{1}{60}n(n+1)(n+2)(3n^2+6n+1)$$

(v) $\sum_{i=1}^{n}(\frac{1}{T_i})$

Solution.

$$\sum_{i=1}^{n}\left(\frac{1}{T_i}\right) = \sum_{i=1}^{n}\frac{2}{i\cdot(i+1)}$$
$$= \frac{2n}{n+1}$$

(b) (i) Under what conditions will T_i be odd?

Solution. T_i will be odd if $i \mod 4 \equiv 1$ or 2.

(ii) Prove that when represented in base ten, no triangular number will end in 4 or 7.

Proof. Recall that every T_i is of the form $\frac{n(n+1)}{2}$. We will proceed by contradiction. Suppose to the contrary that $\frac{n(n+1)}{2} \mod 10 \equiv 4$ and $\frac{n(n+1)}{2} \mod 10 \equiv 7$. First:

$$\frac{n(n+1)}{2} \mod 10 \equiv 4.$$

Then we have the following:

$$\begin{aligned} \frac{n(n+1)}{2} &\mod 10 \equiv 4 \\ n(n+1) &\mod 10 \equiv 8 \\ n \mod 10 \cdot (n+1) &\mod 10 \equiv 8 \\ n \mod 10 \cdot n \mod 10 + 1 &\mod 10 \equiv 8 \\ n \mod 10 \cdot n &\mod 10 \equiv 7 \\ n^2 &\mod 10 \equiv 7 \end{aligned}$$

I claim we have reached a contradiction, since n^2 cannot end in 7. Next, suppose the following:

$$\frac{n(n+1)}{2} \mod 10 \equiv 7.$$

Similarly, we have:

$$\begin{aligned}\frac{n(n+1)}{2} &\mod 10 \equiv 7\\ (n^2+1) &\mod 10 \equiv 4\\ n^2 \mod 10 + 1 &\mod 10 \equiv 4\\ n^2 &\mod 10 \equiv 3\end{aligned}$$

Again, I claim we've reached a contradiction, because n^2 cannot end in 3. $\square$

(c) Prove that every *even* perfect number is a triangular number.

Proof. Let p be a perfect number. Then $p = 2^{k-1} \cdot (2^k - 1)$. Let $n = 2^k - 1$, then:

$$2^{k-1} = \frac{2^k}{2} = \frac{n+1}{2}.$$

Then we have $p = \frac{n+1}{2} \cdot n = \frac{n \cdot (n+1)}{2}$. Since every T_i is of the form $\frac{n \cdot (n+1)}{2}$ for some $n \in \mathbb{N}$, we have shown that p is a triangular number. $\square$

(4) In this problem *Primitive* Pythagorean Triples will be denoted (a, b, c) where a is even and $a^2 + b^2 = c^2$, and Pythagorean Triples will be denoted (x, y, z) where $x < y$ and $x^2 + y^2 = z^2$.

(a) (i) Prove that there is *no* Primitive Pythagorean Triple having

$$c \equiv 3 \mod 4$$

Proof. I claim that every primitive pythagorean triple (a, b, c) is of the form:

$$(a, b, c) = \left(\frac{m^2 - n^2}{2}, mn, \frac{m^2 + n^2}{2}\right)$$

for some pair of relatively prime *odd* numbers $1 \leq n < m$.
Given $a^2 + b^2 = c^2$, we can rewrite this equation as $b^2 = c^2 - a^2$ and factor the right side. Now we have:

$$\begin{aligned}b^2 &= (c+a) \cdot (c-a)\\ 1 &= \left(\frac{c}{b} + \frac{a}{b}\right) \cdot \left(\frac{c}{b} - \frac{a}{b}\right)\end{aligned}$$

Since we have 1 on the left, the two terms on the right must be reciprocals of one another.
Let $\frac{m}{n} = \frac{c}{b} + \frac{a}{b}$ and $\frac{n}{m} = \frac{c}{b} - \frac{a}{b}$. Now we have:

$$\frac{c}{b} = \frac{1}{2} \cdot \left(\frac{m}{n} + \frac{n}{m}\right) = \frac{m^2 + n^2}{2mn}$$

and
$$\frac{a}{b} = \frac{1}{2} \cdot \left(\frac{m}{n} - \frac{n}{m}\right) = \frac{m^2 - n^2}{2mn}$$
From this we can find that $a = \frac{m^2-n^2}{2}$, $b = mn$, and $c = \frac{m^2+n^2}{2}$.

Now we will show that there is no Primitive Pythagorean Triple having $c \equiv 3 \mod 4$. Suppose on the contrary that:
$$c \mod 4 = \frac{m^2+n^2}{2} \mod 4 \equiv 3.$$
Then:
$$\begin{aligned} \frac{m^2+n^2}{2} &\mod 4 \equiv 3 \\ m^2+n^2 &\mod 4 \equiv 2, \end{aligned}$$
which implies that there exists some $i, j \in \mathbb{Z}$ such that $m = 2i$ and $n = 2j$. I claim that we have reached a contradiction, because m, n must be odd. □

(ii) What is the Pythagorean Triple having smallest z such that
$$z \equiv 3 \mod 4$$

Solution. $(9, 12, 15)$, since $15 \equiv 3 \mod 4$.

(b) (i) Prove that there is *no* Primitive Pythagorean Triple having
$$c \equiv 11 \mod 20$$

Proof. We've shown in (4)(a)(i) that primitive pythagorean triples are of the form:
$$(a, b, c) = \left(\frac{m^2-n^2}{2}, mn, \frac{m^2+n^2}{2}\right)$$
Suppose on the contrary that:
$$c \mod 20 = \frac{m^2+n^2}{2} \mod 20 \equiv 11.$$
Then we have that:
$$\begin{aligned} \frac{m^2+n^2}{2} &\mod 20 \equiv 11 \\ m^2+n^2 &\mod 20 \equiv 2, \end{aligned}$$
which implies that there exists some $i, j \in \mathbb{Z}$ such that $m = 2i$ and $n = 2j$. I claim that we have reached a contradiction, because m, n must be odd. □

(ii) What is the Pythagorean Triple having smallest z-value such that

$$z \equiv 11 \mod 20$$

Solution. $(24, 45, 51)$, since $51 \equiv 11 \mod 20$.

(c) We say that a Primitive Pythagorean Triple is *simple* when $a = c-1$. Noting that $(4, 3, 5)$ is the *first* simple triple, that is, 5 is the *smallest* c-value, what is the *simple* triple that has the 100th smallest c-value?

Solution. $(20200, 201, 20201)$.

(d) As pointed out in class Primitive Pythagorean Triples may be listed according to the values of t and s where $t > s$, $\gcd(t, s) = 1$, and $s \not\equiv t \mod 2$. As examples, the first 4 primitive triples have $(t, s) = (2, 1), (3, 2), (4, 1)$, and (4,3) respectively. $(a, b, c) = (4, 3, 5), (12, 5, 13), (8, 15, 17)$, and $(24,\ 7,\ 25)$.

(i) In what position on the list will the 10th *simple* triple appear?

Solution. The tenth simple triple is the 27th primitive pythagorean triple.

(ii) If L_i denotes the position of the ith simple triple on the list, explain why $L_{2i+1} - L_{2i}$ is *even*, $i \geq 1$.
For example, when $i = 1$, $L_3 - L_2 = 4 - 2$.
Note also that $L_5 - L_4 = 8 - 6$.

(e) Let q be a *prime number* such that $q \equiv 3 \mod 4$. $(q = 3, 7, 11, 19, \ldots)$
Prove that *no* primitive triple has $c \equiv 0 \mod q$.
Hint: Consider the *group* $U(q)$. Note that $|U(q)| = \phi(q) = q-1$. Use results from group theory.

(5) In this problem you will consider integer solutions to the equation $x^2 + y^2 = z^4$. We shall refer to a solution of this equation as a Trinity triple. Moreover, if (x, y, z) is a Trinity triple such that $\gcd(x, y, z) = 1$, it shall be called primitive.

(a) Prove that if (a, b, c) is a primitive Trinity triple, then a, b, or c is divisible by 5.

Proof. Obviously $a, b \mod 5 = 0, 1, 2, 3, \text{or } 4$. Therefore, $a^2, b^2 \mod 5 = 1 \text{ or } 4$. Hence, $c \equiv (1+1) \mod 5$, $c \equiv (1+4) \mod 5$, or $c \equiv (4+4) \mod 5$.
Additionally, $c \mod 5 = 0, 1, 2, 3, \text{or } 4$. Therefore, $c^4 \mod 5 = 0$ or 1.
We now know that $c^4 \not\equiv (1+1) \mod 5$, since $2 \mod 5 \neq 0$ or 1. Similarly, $c^4 \not\equiv (4+4) \mod 5$, since $3 \mod 5 \neq 0$ or 1.
Therefore, the only solutions to $a^2 + b^2 = c^4$ have one of a, b being equivalent to $1 \mod 5$ and the other being equivalent to $4 \mod 5$. In this situation, $c^4 \mod 5 \equiv 0$, which means that c^4 is divisible by 5. $\square$

(b) Let (a,b,c) be a primitive Trinity triple of $a^2 + b^2 = c^4$.

(i) Prove that if $b \equiv 3$ or $7 \mod 10$, then c is divisible by 5 and $a \equiv 4$ or $6 \mod 10$.

(ii) Give an example of a primitive Trinity triple that meets the conditions in (b)(i).

(c) Observing that if (a, b, c) is a primitive Trinity triple, then (a, b, c^2) is a primitive Pythagorean triple, use the results of primitive Pythagorean triples (values of s and t) to demonstrate a one-to-one correspondence between the set of primitive Pythagorean triples and the set of primitive Trinity triples.