Midterm 1 Solutions

February 5, 2012

Problem 1

The check digit of 3946022518 is a number r where $0 \leq r \leq 8$ and $3946022518 \equiv r \bmod 9$. We can find the remainder of this number mod 9 by adding the digits:

$$3946022518 \equiv 3+9+4+6+0+2+2+5+1+8 \equiv 40 \equiv 4 \bmod 9$$

so the check digit is 4.

Problem 2

We need to find two elements $x \in U(999) = \{a \in \mathbb{N} \,|\, a < 999 \,\&\, \gcd(a, 999) = 1\}$ such that $x^2 = 1$, the identity element of $U(999)$.

Let us forget about modular arithmetic for a moment and solve $x^2 = 1$ with algebra: $x = 1$ and $x = -1$. $x = 1 \in U(999)$ ($\gcd(1, 999) = 1$), but $-1 \notin U(999)$ since -1 is not a natural number. Here, we need modular arithmetic to replace $x = -1$ by a number between 0 and 998. Since

$$-1 \equiv 998 \bmod 999$$

we can try $x = 998$ as our other solution. But we're not done yet - is $998 \in U(999)$? That is, is $\gcd(998, 999) = 1$? We can answer this in two ways:

Divisors of 999, 998, and their Difference

Suppose d is a positive integer that divides both 999 and 998. Then d must divide $999 - 998 = 1$. The only positive number that can do this is $d = 1$, so 1 is the only common divisor of 999 and 998. It must be their greatest common divisor.

Euclidean Algorithm

For the first step of the Euclidean algorithm, we will use $a = 999$ and $b = 998$. Then we have

$$999 = (998)(1) + 1$$

Next, we use the algorithm again with $a = 998$ (the previous value of b) and $b = 1$ (the remainder from the previous line)

$$998 = (1)(998) + 0$$

The last nonzero remainder when using the Euclidean algorithm is 1, so $1 = \gcd(999, 998)$.

Either way, since $\gcd(999, 998) = 1$, $998 \in U(999)$ and $998^2 \equiv (-1)^2 \equiv 1 \bmod 999$. Thus, our two solutions are $x = 1$ and $x = 998$.

Problem 3

With Induction

Base case $n = 1$:

$$3^1 2^3 - 1 \bmod 23 = 24 - 1 \bmod 23 = 23 \bmod 23 = 0 \bmod 23$$

Suppose the statement is true for $n = k$. That is,

$$3^k 2^{3k} - 1 \bmod 23 = 0 \bmod 23$$

Let us plug in $n = k + 1$ on the left hand side and try to factor it:

$$3^{(k+1)} 2^{3(k+1)} - 1 \bmod 23 = 3^1 2^3 (3^k 2^{3k}) - 1 \bmod 23$$
$$= 24(3^k 2^{3k}) - 1 \bmod 23$$

There are a few ways to proceed.

1. Split $24 = 23 + 1$ and use the fact that multiples of 23 are congruent to zero mod 23:

   $$= (23 + 1)\left(3^k 2^{3k}\right) - 1 \bmod 23 = 23(3^k 2^{3k}) + 3^k 2^{3k} - 1 \bmod 23 = 0 + 3^k 2^{3k} - 1 \bmod 23$$

   By the inductive hypothesis, this equals zero mod 23.

2. Since $23 = 0 \bmod 23$, we can safely subtract 23 without changing anything (it is as if we were adding zero):

   $$24(3^k 2^{3k}) - 1 - 23 \bmod 23 = 24(3^k 2^{3k}) - 24 \bmod 23 = 24(3^k 2^{3k} - 1) \bmod 23$$

   After factoring out 24, we use the inductive hypothesis to get $24(0) \bmod 23 = 0 \bmod 23$.

This proves the statement for $n = k + 1$. Therefore, by induction, the statement is true for any natural number n.

Without Induction

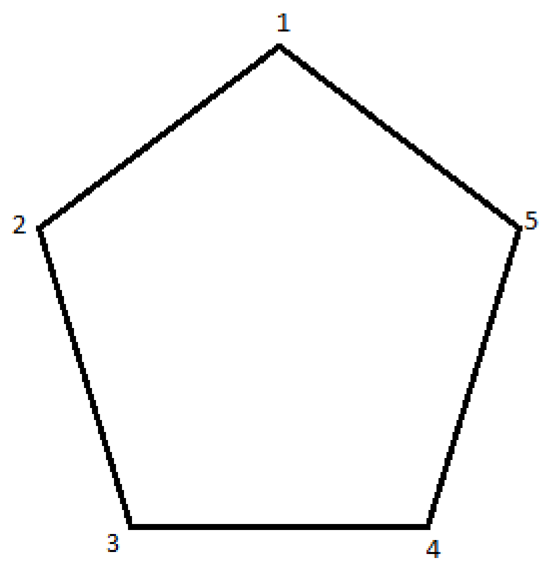
We use the fact that $24 \bmod 23 = 1 \bmod 23$:

$$3^n 2^{3n} - 1 \bmod 23 = \left(3 \cdot 2^3\right)^n - 1 \bmod 23 = 24^n - 1 \bmod 23 = 1^n - 1 \bmod 23 = 0 \bmod 23$$

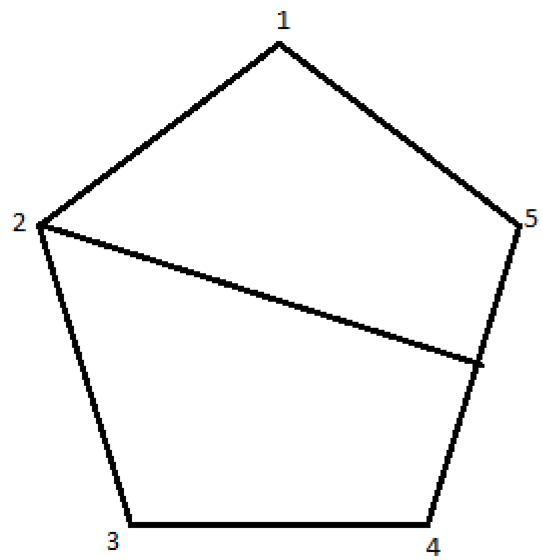
Problem 4

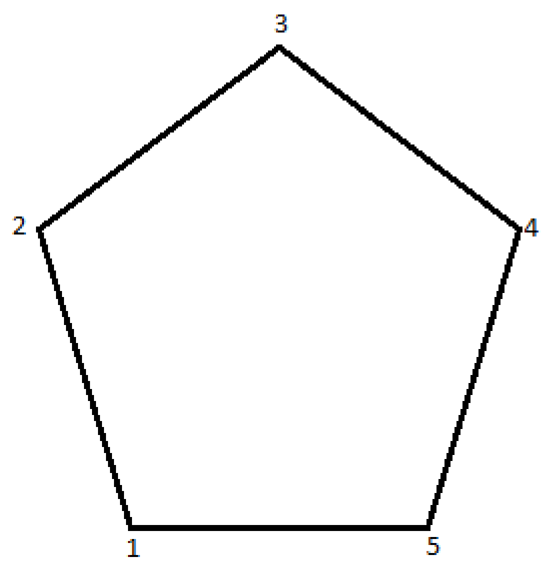
Let us draw what each reflection does. Remember, $F_1 F_2$ means F_2 first, then F_1 second - in D_5 and any group whose group operation is function composition, we read from right to left.

Label the vertices counter-clockwise. 1 is the top vertex.

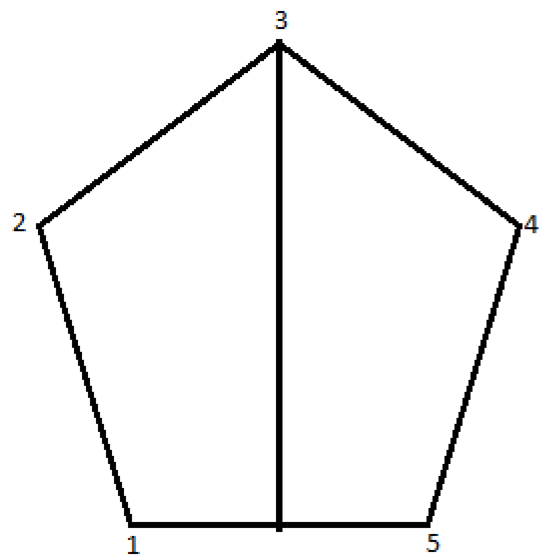


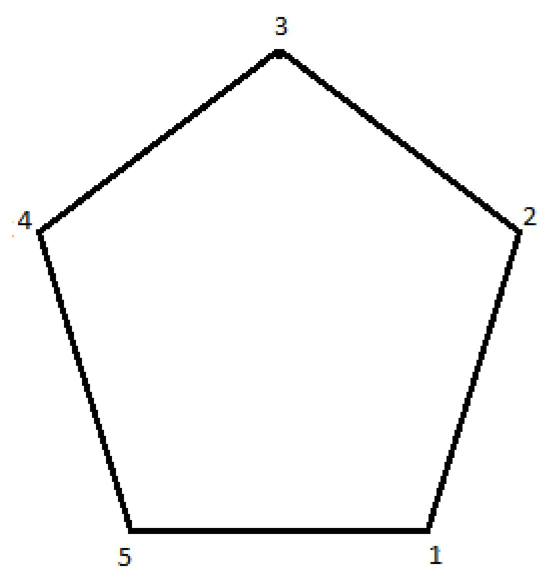
Do F_2 first. That is a reflection across a line through where vertex 2 starts.





Now we apply F_1. This is a reflection about a line through the original location of vertex 1 - the top vertex.





We see that the end result is a rotation - notice that the labels go up counter-clockwise. To determine how many degrees we rotated the pentagon counter-clockwise, we take 360, divide it by 5, then multiply by 3 (since vertex 1 moves three places counter-clockwise). Thus, F_1F_2 is rotation by 216 degrees counter-clockwise.

Problem 5

The Cayley Table

Let $M_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, where $a \in \mathbb{Z}_4 = \{0, 1, 2, 3\}$, a group whose operation is addition mod 4. Then

$$M_a M_b = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$$

For example,

$$M_1 M_2 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$$

$$M_2 M_3 = \begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \bmod 4$$

Here is the table:

	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$

The Order of $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$

Now let us compute the order of $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$. First, $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (look in the table). Since $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ raised to the second power is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the identity element of G, the order of $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ must be 2.

Problem 6

Using Linear Combinations

To show that $\gcd(7n+4, 2n+1) = 1$, we need to find integers s and t such that $s(7n+4) + t(2n+1) = 1$. Let us expand the left hand side:

$$7sn + 4s + 2tn + t$$

Put the terms being multiplied by n together:

$$n(7s + 2t) + 4s + t$$

We want this to equal 1, so we need to get rid of n. We can do this by requiring that

$$7s + 2t = 0$$

If that is the case, then all that is left over is $4s + t$. We want this to equal 1:

$$4s + t = 1$$

Thus, s and t are integers that must satisfy the system of equations

$$7s + 2t = 0$$

$$4s + t = 1$$

We can solve this by multiplying the second equation by 2 and subtracting it from the first equation to get

$$-s = -2$$

$$s = 2$$

Therefore,

$$t = -7$$

Let's plug these in:

$$(2)(7n + 4) + (-7)(2n + 1) = 14n + 8 - 14n - 7 = 1$$

Thus, we can find integers s and t so that $s(7n+4)+t(2n+1) = 1$. This means that the greatest common divisor of $7n + 4$ and $2n + 1$ is at most 1. So it must be 1.

Using the Euclidean Algorithm

$$7n + 4 = (2n + 1)(3) + (n + 1)$$

$$2n + 1 = (n + 1)(1) + n$$

$$n + 1 = (n)(1) + 1$$

$$n = (1)(n)$$

Thus, $\gcd(7n + 4, 2n + 1) = 1$ for any positive integer n.