Mann, Isaiah
Section 1
Homework 6
Due: 10/31/14

1.a. *Given that a|b and b|c , prove that a|c .*

if a|b, $am_1=b$
if b|c, $bm_2 = c$
$bm_2 = c$
(substitute am_1 for b)
$am_1m_2 = b$
$m_1m_2 \in \mathbb{Z}$
$m_1m_2 = p$ (integer)
$a \in \mathbb{Z}$
Therefore, $ap = c$
Because integer a times integer p equals integer c, a|c

1.b. *Given that a|b and c|d , prove that (ac)|(bd) .*

if a|b, $am_1 = b$
if c|d, $cm_2 = d$
(ac)|(bd)
(substitute alternate forms)
(ac)|(am_1cm_2)
if (ac)|(am_1cm_2), $acn = am_1cm_2$
$acn = am_1cm_2$
(divide both sides by ac)
$n = m_1m_2$
$n \in \mathbb{Z}$
(because $\mathbb{Z}$ is closed under multiplication)
Therefore, because ac can multiply by an integer to equal bd,
(ac)|(bd)

1.c *Given that a|b and a|c , prove that a|(b − c) .*

if $a|b$, $am_1=b$

if $a|c$, $am_2 = c$

$a|(b - c)$

(substitute all terms for versions containing a)

$a|(am_1 - am_2)$

(factor out a)

$a|a(m_1 - m_2)$

$m_1 - m_2 \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under subtraction

Therefore, because a times integer $(m_1 - m_2)$ equals $a|(b - c)$, a must divide $(b - c)$

1.d. *Given that a divides b with remainder r and that a divides c with remainder (a − r) , prove that a|(b + c).*

Given: $a|(b - r)$

$a|(c - (a - r))$

If $a|(b - r)$, $am_1 = b - r$

If $a|(c - (a - r))$, $am_2 = c - (a - r)$

$b + c =$

$am_1 + r + am_2 + a - r =$

$am_1 + am_2 + a =$

$a(m_1 + m2_2 + 1) = (b + c)$

Therefore, because a, m_1, m_2, and 1 are integers and $\mathbb{Z}$ is closed under addition and multiplication, $a|(b + c)$

2. *Show that the set of rational numbers, $\mathbb{Q}$, is closed under addition*

If $n \in \mathbb{Q}$, $n = p/q$, where $p \& q \in \mathbb{Z}$

If $m \in \mathbb{Q}$, $n = r/s$, where $r \& s \in \mathbb{Z}$

$n + m$

(convert to ratio of two integers)

$p/q + r/s$

(multiply by identity to give the ratios of the same denominator)

$ps/qs + rq/qs$

(ps + rq)/qs
Because $\mathbb{Z}$ is closed under Multiplication and addition
(ps + rq) and qs $\in \mathbb{Z}$
Therefore, n + m is a ratio of two integers and (n + m) $\in \mathbb{Q}$, meaning that $\mathbb{Q}$ is closed under addition

3. *Let L denote the set of all subsets {1, 2, 3, …, n} that contain no two consecutive integers*

3.a. Is L closed under the union operation? If yes, prove it. If no, given an example of an application of the union operation that "Leaves" L.

No.
{1, 3}, {2, 4} $\in$ L, {1, 3} $\cup$ {2, 4} = {1, 2, 3, 4} $\notin$ L

3.b. Is L closed under the intersection operation? If yes, prove it. If no, given an example of an application of the intersection operation that "Leaves" L.

Yes.
If A, B $\subseteq$ L
A $\cap$ B $\subseteq$ L
If x $\in$ A and x $\notin$ B, then x $\notin$ A $\cap$ B
If x $\in$ A, B, then x $\in$ A $\cap$ B
Any x that is an element of A & B is at least +/− 2 away from any element in both subsets, therefore there are no terms in the intersection that are consecutive, and A $\cap$ B $\subseteq$ L

4. *For k$\in$N, let M_k denote the set {n$\in$N : k|n}*

4.a Find a prime factorization for 365

73 * 5 = 365

4.b. Express M_{365} as an intersection of some M_k s

$M_{73} \cap M_5 = M_{365}$

4.c. For q$\in$N, prove that $M_{(365 * q)} \subseteq M_{365}$

That is, show that every element in $M_{(365 * q)}$ is also in M_{365}.

$M_{(365 * q)} = M_{365} \cap M_q$

Therefore, by the definition of intersection, all elements included in $M_{(365 * q)}$ are also in M_{365}

4.d. If p is a prime factor of c, prove that M_c is a subset of M_p

$p = c * x$

Where $x \in \mathbb{Z}$

$M_p = M_c \cap M_x$

Therefore, by the definition of intersection, $M_p \subseteq M_c$

5. *For prime p, prove that* $\sqrt{p} \notin \mathbb{Q}$

Proof by contradiction:

- Assume that $\sqrt{p} \in \mathbb{Q}$

  Therefore, $\sqrt{p}$ can be expressed as the ratio of two integers

  $r/s = \sqrt{p}$: r, $s \in \mathbb{Z}$

  $r^2/s^2 = p$

  $r^2 = ps^2$

  n = the number of p's in the prime factorization of r

  m = the number of p's in the prime factorization of s

  $2n = 2m + 1$

  $2n \neq 2m + 1$

  (this term cannot be both an odd and an even number)

  Therefore, the assumption is false

  Proving that $\sqrt{p} \notin \mathbb{Q}$

  ∎

6. (10 points) Assume that x is a composite number. Let p ˘denote the smallest prime factor of x . Claim: p ˘≤√x.

If x is composite, ∃ m/p ˘= x , m∈ℤ

$p \breve{} \leq \sqrt{x}$

$p \breve{} \leq \sqrt{mp \breve{}}$

Where m ∈ ℤ

p ˘2 ≤ mp ˘

p ˘≤ m

This is a true inequality, because p ˘is the smallest prime factor of x, therefore, m is either equal to p ˘, or a larger factor. This proves that the smallest prime factor of a composite number is less than its square root.

∎

7. (12 points) Return again to random.org.

(a) Generate a random realization x from the uniform distribution on {1, 2, 3, ..., 100} and record how many numbers in the set {1, 2, 3, ..., 10} divide it. Do this 10 times. What was the average number of divisors from {1, 2, 3, ..., 10} in the trials you conducted?

Trial #	x	# of divisors
1	39	2
2	67	1
3	88	4
4	33	2
5	51	2
6	30	6
7	7	2
8	7	2
9	84	6
10	93	2

Average number of divisors: 3.7

(b) Consider a value function v that is 1 if 2|x and 0 otherwise. What is the expectation of this function if x is chosen from the uniform distribution between 1 and 100? How would your answer change if instead v was is 1 if 3|x and 0 otherwise?

If 2|x, expectation is 0.5 = (1 * 50 + 0 * 50)/100
If 3|x, expectation is 0.33 = (1 * 33 + 0 * 67)/100

(c) For the experiment you conducted in (a): compute the expected number of divisors x has from the set {1, 2, 3, ..., 10} . (This computation does not need to be highly accurate, but make sure that your reasoning is clear.) How does what you found empirically in (a) compare to the expectation you computed?

Number of values divisible by 1 = 100
Number of values divisible by 2 = 50
Number of values divisible by 3 = 33
Number of values divisible by 4 = 25
Number of values divisible by 5 = 20
Number of values divisible by 6 = 16
Number of values divisible by 7 = 14
Number of values divisible by 8 = 12
Number of values divisible by 9 = 11
Number of values divisible by 10 = 10
(100 + 50 + 33 + 25 + 20 + 16 + 14 + 12 + 11 + 10)/100 = 2.91
My calculated value was a great deal higher than the expected number of divisors (which was achieved by summing how many multiples each divisor has within the set of {1, 2, 3, ..., 99, 100}

However, with a greater number of iterations, I expect the average number of divisors to come roughly in line with 2.91

8. *Let p denote a prime number larger than 3. Since p is prime, if we attempt to divide p by 6 we will get some remainder between 1 and 5. Prove the following:*

(a) Claim:If 6|(p−r) then either r=1 or r=5.

For every twenty four consecutive integers, there are 5 multiples of six, ending in six, two, eight, four or zero progressively.

All prime numbers end in 1, 3, 7, or 9.

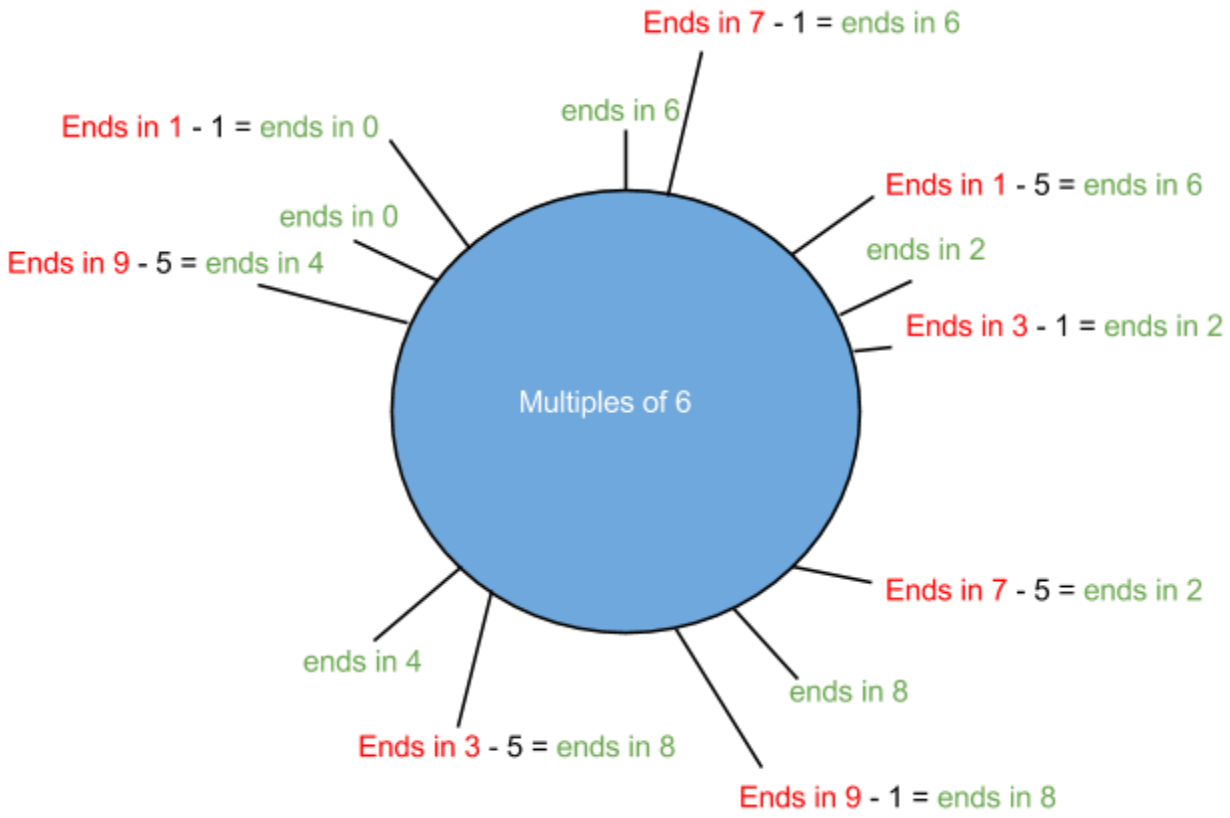
Cases for what digit the prime ends with:

For 1, subtract 1 and you get a number that ends in 0, or subtract 5 and you get a number that ends in 6.

For 3, subtract 1 and you get a number that ends in 2, or subtract 5 and you get a number that ends in 8.

For 7, subtract 1 and you get a number that ends in 6, or subtract 5 and you get a number that ends in 2.

For 9, subtract 1 and you get a number that ends in 8, or subtract 5 and you get a number that ends in 4.



Therefore, you can generalize for any prime n, that because the last digit of six repeats itself every 24 integers, subtracting either one or five from the integer will cause it to equal a multiple of 6.

(b) Claim: If j is a natural number greater than 3, then at least one element of the set {j,j+2,j+4} is not prime.(Hint:use(a)).

Case A: j is not prime. Therefore the condition is true by default.

Case B: j is prime, by adding two, you now have a number that ends in 3, 5, 9, or 1, any term ending in a 5 is divisible by 5.

Case C: if j and j+2 are prime, then j + 4 cannot be prime. There are no three primes (apart from 3, 5, and 7) that can be achieved consecutively by adding 2 to the previous term. Due to the inclusion of 3 as a divisor, there can only every by 2 primes in a row with a difference of 2.