Building Blocks Homework 5
Solution

Question A) Prove that if a|b and a|c then a|(b+c) for positive integers a, b, c.

Given: a|b
a|c
Show: a|(b+c)
By definition a|b means that b=ak for some integer k.
Similarly a|c means that c=aj for some integer j.
Consider b+c = ak+aj = a(k+j). We know that k+j is an integer and therefore a divides b+c.
QED

Question B) Use Euclid's algorithm to find the GCD of the following pairs of values. Show the recursive calls made.

a) 44, 16
b) 100, 97
c) 132, 60

```
procedure gcd(a,b)
     r := remainder(a,b)
     if (r = 0) return b
     else return gcd(b,r)
```

a) gcd(44,16)
   r= remainder(44, 16) = 12
   gcd(16,12)
   r= remainder(16, 12) = 4
   gcd(12,4)
   r= remainder(12, 4) = 0
   return 4

b) gcd(100,97)
   r= remainder(100, 97) = 3
   gcd(97,3)
   r= remainder(97, 3) = 1
   gcd(3,1)
   r= remainder(3, 1) = 0
   return 1

c) gcd(132,60)
   r= remainder(132, 60) = 12
   gcd(60,12)
   r= remainder(60, 12) = 0
   return 12

Question C) Are any of the pairs of values in the previous problem relatively prime?

A pair of values is relatively prime if they share no prime factors and this happens if the GCD is 1. Only the pair 100,97 are relatively prime from the last problem.

Question D) Compute the following values

a) $(12543 \times 388^{201}) mod_2$

b) $(8^{101}) mod_9$

c) $\left(4 \times 2^{30} + 4^4 \times 10^{50} + 20^{100^{100}}\right) mod_4$

d) $(312321 \times 440063 \times 288 \times 2422) \text{mod}_{10}$

e) $(2001! + 31123112! + 1) mod_{200}$

$(12543 \times 388^{201}) mod_2$

$= (12543 \times (388 mod_2)^{201}) mod_2$

$= (12543 \times (0)^{201}) mod_2$

$= 0\ mod_2$

$= 0$

$(8^{101}) mod_9$

$= (8 \times (8^2)^{50}) mod_9$

$= (8 \times (8^2 mod_9)^{50}) mod_9$

$= (8 \times (1 mod_9)^{50}) mod_9$

$= (8 \times 1^{50}) mod_9$

$= (8) mod_9$

$= 8$

$\left(4 \times 2^{30} + 4^4 \times 10^{50} + 20^{100^{100}}\right) mod_4$

$= \left(4 mod_4 \times 2^{30} + 4 mod_4{}^4 \times 10^{50} + 20 mod_4{}^{100^{100}}\right) mod_4$

$= \left(0 \times 2^{30} + 0^4 \times 10^{50} + 0^{100^{100}}\right) mod_4$

$= 0$

$(312321 \times 440063 \times 288 \times 2422) \text{mod}_{10}$

$= (312321 \text{mod}_{10} \times 440063 \text{mod}_{10} \times 288 \text{mod}_{10} \times 2422 \text{mod}_{10}) \text{mod}_{10}$

$= (1 \times 3 \times 8 \times 2) \text{mod}_{10}$

$= (48) \text{mod}_{10}$

$= 8$

$(2001! + 31123112! + 1) mod_{200}$

$= (0 + 0 + 1) mod_{200}$ (Both factorials have 200 as a factor.)

$= 1$

Question E) Give a direct proof of the following statement.
For all integers n, m, if n is odd and m is odd, then $(n+1)m^2 + m$ is odd. Use the following definition of even/odd

Even: Integer n is even iff n mod2 = 0
Odd: Integer n is odd iff n mod2 = 1

Give: **n is odd**
m is odd
Show: $\boldsymbol{(n+1)m^2 + m}$ **is odd**

Since n is odd we know that $nmod_2 = 1$
Since m is odd we know that $mmod_2 = 1$

$Consider((n+1)m^2 + m)mod_2$
We apply the mod to n and m inside.

$$= \left((nmod_2+1)mmod_2{}^2 + mmod_2\right)mod_2$$

And replace each

$$= ((1+1)1^2 + 1)mod_2$$
$$= ((1+1)1^2 + 1)mod_2$$
$$= (2 + 1)mod_2$$
$$= 1$$

Therefore, $(n+1)m^2 + m$ is odd
QED

Question F) Give proof by cases of the following statement.

For all integers n, $(n^2 - n) \times 2n$ is divisible by 4.

(Hint: You should have 4 cases.)

Divisible by 4: Integer n is divisible by 4 iff n mod4 = 0

The four cases are $nmod_4 = 0; nmod_4 = 1;\ nmod_4 = 2;\ nmod_4 = 3$

For each case we want to show that:

$$\big((n^2 - n) \times 2n\big)mod_4 = 0$$

Which can be rewritten as

$$\Big(\big(nmod_4{}^2 - nmod_4\big) \times 2 \times nmod_4\Big)\, mod_4 = 0$$

Case 0: $nmod_4 = 0$

$$\Big(\big(nmod_4{}^2 - nmod_4\big) \times 2 \times nmod_4\Big)\, mod_4$$
$$= \big((0^2 - 0) \times 2 \times 0\big)mod_4$$
$$= 0mod_4$$
$$= 0$$

Case 1: $nmod_4 = 1$

$$\Big(\big(nmod_4{}^2 - nmod_4\big) \times 2 \times nmod_4\Big)\, mod_4$$
$$= \big((1^2 - 1) \times 2 \times 1\big)mod_4$$
$$= 0mod_4$$
$$= 0$$

Case 2: $nmod_4 = 2$

$$\Big(\big(nmod_4{}^2 - nmod_4\big) \times 2 \times nmod_4\Big)\, mod_4$$
$$= \big((2^2 - 2) \times 2 \times 2\big)mod_4$$
$$= 8mod_4$$
$$= 0$$

Case 3: $nmod_4 = 3$

$$\Big(\big(nmod_4{}^2 - nmod_4\big) \times 2 \times nmod_4\Big)\, mod_4$$
$$= \big((3^2 - 3) \times 2 \times 3\big)mod_4$$
$$= 36mod_4$$
$$= 0$$

Question G) Show $(3^{11})mod_5$ is not the same as $(3^{11mod_5})mod_5$

$$(3^{11})mod_5 = (3^4 \times 3^4 \times 3^3)mod_5$$
$$= (81 \times 81 \times 27)mod_5$$
$$= (1 \times 1 \times 2)mod_5$$
$$= 2$$

$$(3^{11mod_5})mod_5 = (3^1)mod_5$$
$$= 3$$

You may choose to solve one (and only one) of the following Extra Credit Problems. If you submit more than one, only the first will be graded.

Extra Credit 1)
Suppose that you want to compute $a^n mod_m$ when n is large. One way to do this is given by the following algorithm

```
def a-to-n(a, n, m):
     result = 1;
     for i in range(0,n):
          result = (result*a) % m
     return result
```

The problem with this algorithm is that it requires n multiplications.

We can do this faster by noting that $a^{2k} mod_m = (a^k)^2 mod_m$ so if the exponent is even we compute $a^k mod_m$ and square the result. We do something similar if the exponent is odd. Write a program that uses this technique and compare answers with the given algorithm.

```
def a-to-n(a, n, m):
     if n==0: return 1
     halves = a-to-n(a, n//2, m)
     if n%2 == 0:
          #Even
          return halves**2 % m
     else:
          #Odd
          return (halves**2*a) % m
```

Extra Credit 2) Prove that if the digits of an integer value n add up to a value that is divisible by 3, then n is also divisible by 3. Prove that if the digits of an integer value n add up to a value that is divisible by 9, then n is also divisible by 9.

Consider the decimal expansion of a number

$$n = a_0 + a_1 10^1 + a_2 10^2 + a_3 10^3 + a_4 10^4 + \ldots + a_n 10^n$$

If we mod this by 3 we get

$$(a_0 + a_1 10^1 + a_2 10^2 + a_3 10^3 + a_4 10^4 + \ldots + a_n 10^n) mod_3$$

And this will be divisible by three if the result is zero. Observe that 10mod3 is 1, so we can replace all the 10s by 1s

$$(a_0 + a_1 1^1 + a_2 1^2 + a_3 1^3 + a_4 1^4 + \ldots + a_n 1^n) mod_3$$

Or

$$(a_0 + a_1 + a_2 + a_3 + a_4 + \ldots + a_n) mod_3$$

Which is just the sum of the digits

Similarly, if we check for divisibility by 9, we look at

$$(a_0 + a_1 10^1 + a_2 10^2 + a_3 10^3 + a_4 10^4 + \ldots + a_n 10^n) mod_9$$

And 10 mod 9 = 1

$$(a_0 + a_1 1^1 + a_2 1^2 + a_3 1^3 + a_4 1^4 + \ldots + a_n 1^n) mod_9$$

Or

$$(a_0 + a_1 + a_2 + a_3 + a_4 + \ldots + a_n) mod_9$$

Which is just the sum of the digits again.