Fleck Chapter 4 – A tiny taste of number theory.

Problem 1 Are the following true or false?

a) 1 | 5,
b) 3 | 18
c) 10 | 0
d) 55 | 5

a) 1 | 5,

1 divides 5 if we can find some integer k, where 1xk = 5. The value of k is 5. So true.

b) 3 | 18

3 divides 18 if we can find some integer k, where 1x3 = 18. The value of k is 6. So true.

c) 10 |

0 10 divides 0 if we can find some integer k, where 10xk = 0. The value of k is 0. So true.

d) 55 | 5

55 divides 5 if we can find some integer k, where 55xk = 5. No integer value works, So false.

Problem 2
Prove that if $a|b$ and $c|b$ then $ac|b^2$ for integers a, b, c, $a\neq 0$, $c\neq 0$

Given:

a divides b
c divides b
$a\neq 0$, $c\neq 0$

Show:

ac divides b^2

Proof:

a divides b means we can write $b=na$ for some integer n.
c divides b means we can write $b=mc$ for some integer m.

Consider b^2. We can write it as $b^2=(na)(mc) = (nm)(ac)$.
Since nm is an integer, we have what we need to show that ac divides b^2
QED.

Problem 3 Give a counterexample to show that if $a|b$ and $c|b$ then $ac|b^2$ for integers a, b, c, $a\neq 0$, $c\neq 0$ need not be true.

Let $a=3$ and $b=24$. We know that 3 divides 24
Let $c=6$ and $b=24$. We know that 6 divides 24

But $ac=(3)(6)=18$ does not divide 24.
QED.

Problem 4 Give prime factorizations of the following numbers.

a) 2
b) 24
c) 123
d) 54

a) 2
   2 = 2 (If the value is prime, just list it.)
b) 24
   24 = 2x2x2x3
c) 123
   123 = 3x41
d) 54
   54 = 2x3x3x3

Problem 5 Use Euclid's algorithm to find the GCD of the following pairs of values. Show the recursive calls made.

a) 312, 10
b) 325, 75
c) 134, 432

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

a) 312, 10
   gcd(312, 10), Compute r =rem(312,10) =2
   gcd(10, 2), Compute r =rem(10,2) =0
   return 2

b) 325, 75
   gcd(325, 75), Compute r =rem(325,75) =25
   gcd(75, 25), Compute r =rem(75,25) =0
   return 25

c) 134, 432
   gcd(134, 432), Compute r =rem(134,432) =134
   gcd(432, 134), Compute r =rem(432,134) = 30
   gcd(134, 30), Compute r =rem(134,30) = 14
   gcd(30, 14), Compute r =rem(30,14) = 2
   gcd(14, 2), Compute r =rem(14,2) = 0
   return 2

Problem 6 Determine if the following pair of values are relatively prime.

2420, 1911

Relatively Prime: n and m are relatively prime if their prime factorizations share no common factors.

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

We can factor each of the numbers and then compare to see if they share any factors

2420 = 2x2x5x11x11
1911 = 3x7x7x13

They share no prime factors, so they are relatively prime.

The convenient alternative. If the gcd of the numbers is 1, then the numbers share no prime factors

gcd(2420, 1911) : r = rem(2420, 1911) = 509
gcd(1911, 509) : r = rem(1911, 509) = 384
gcd(509, 384) : r = rem(509, 384) = 125
gcd(384, 125) : r = rem(384, 125) = 9
gcd(125, 9) : r = rem(125, 9) = 8
gcd(9, 8) : r = rem(9, 8) = 1
gcd(8, 1) : r = rem(8, 1) = 0
return 1

The mod rules.

If you have a mod, you can freely apply it to the terms inside:

$$\left(x+y\right)\bmod m=(x\bmod m+y)\bmod m$$

If you have a mod, you can freely apply it to the factors inside:

$$\left(xy\right)\bmod m=(y\cdot x\bmod m)\bmod m$$

If you have a mod, you can freely apply it to the base of exponentials inside:

$$\left(x^a\right)\bmod m=\left(\left(x\bmod m\right)^a\right)\bmod m$$

If you have a congruence,

$$x\equiv y\pmod m$$

You can add/subtract the same value from both sides. You can multiply both sides by the same value. Note that you will always have a final mod m that is applied to both sides of the equation.

Problem 7 Compute the following values

a) $\left(12+3^4\right)\bmod 2$

b) $\left(7^{100}\right)\bmod 5$

c) $\left(1^{10}+2^{20}+3^{30}\right)\bmod 3$

d) $\left(11^{13}\right)\bmod 13$ (Since 11 and 13 are relatively prime, I expect that the result will be 11 according to Fermat's Little Theorem.)

a)

$$\begin{aligned}&\left(12+3^4\right)\bmod 2\\&=\left(\left(12\bmod 2\right)+\left(3\bmod 2\right)^4\right)\bmod 2\\&=\left(0+1^4\right)\bmod 2\\&=1\end{aligned}$$

b)

$$\begin{aligned}&\left(7^{100}\right)\bmod 5\\&=\left(\left(7\bmod 5\right)^{100}\right)\bmod 5\\&=\left(2^{100}\right)\bmod 5\\&=\left(\left(2^4\right)^{25}\right)\bmod 5\\&=\left(\left(16\bmod 5\right)^{25}\right)\bmod 5\\&=\left(1^{25}\right)\bmod 5\\&=1\end{aligned}$$

c) $\left(1^{10}+2^{20}+3^{30}\right)\bmod 3$

$$=\left(1+2^{20}+\left(3\bmod 3\right)^{30}\right)\bmod 3$$

$$=\left(1+2^{20}+0^{30}\right)\bmod 3$$

$$=\left(1+2^{20}\right)\bmod 3$$

$$=\left(1+\left(2^{2}\right)^{10}\right)\bmod 3$$

$$=\left(1+\left(4\bmod 3\right)^{10}\right)\bmod 3$$

$$=\left(1+1^{10}\right)\bmod 3$$

$$=2$$

d) $\left(11^{13}\right)\bmod 13$

$$=\left(11\cdot\left(11^{2}\right)^{6}\right)\bmod 13$$

$$=\left(11\cdot\left(121\bmod 13\right)^{6}\right)\bmod 13$$

$$=\left(11\cdot 4^{6}\right)\bmod 13$$

$$=\left(11\cdot\left(4^{2}\right)^{3}\right)\bmod 13$$

$$=\left(11\cdot\left(4^{2}\bmod 13\right)^{3}\right)\bmod 13$$

$$=\left(11\cdot\left(3\right)^{3}\right)\bmod 13$$

$$=\left(11\cdot 27\right)\bmod 13$$

$$=\left(11\cdot 1\right)\bmod 13$$

$$=11$$

Problem 8 Give a proof by cases of the the following statement.
For all integer n, n^2+n is even. 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

We will have two cases: n is even, n is odd
Case 1:
Given:
n is an integer
n is even
Show:
n^2+n is even

Proof:
Since n is even, we know that n mod2 = 0
Consider (n^2+n) mod2
We can write this as $((n \bmod 2)^2+(n \bmod 2)) \bmod 2$
Substitute in zero for n mod2 to get (0^2+0) mod2
Which is zero. Therefore by our definition, we know that n^2+n is even
✓

Case 2:
Given:
n is an integer
n is odd
Show:
n^2+n is even

Proof:
Since n is odd, we know that n mod2 = 1
Consider (n^2+n) mod2
We can write this as $((n \bmod 2)^2+(n \bmod 2)) \bmod 2$
Substitute in one for n mod2 to get (1^2+1) mod2
Is equal to (2) mod2
Which is zero. Therefore by our definition, we know that n^2+n is even
QED

Problem 8 Give a proof by cases of the following statement.
For all integer n, m, if m+n is even then m-n is even.

We will have 4 cases.

1) n,m both even,
2) n,m both odd
3) n even, m odd
4) n odd, m even

Case 1:
Given:
n is an integer
m is an integer
n is even
m is even
Show:
If m+n is even then m-n is even

Proof:
Since n is even, we know that n mod2=0.
Since m is even, we know that m mod2=0.
Consider (m+n) mod2
We can write this as ((m mod2)+(n mod2)) mod2
Is (0+0) mod2 = 0 is even

Consider (m-n)mod2
We can write this as (0-0) mod2=0
Is even. ✓

Case 2:
Given:
n is an integer
m is an integer
n is odd
m is odd
Show:
If m+n is even then m-n is even

Proof:
Since n is odd, we know that n mod2=1.
Since m is odd, we know that m mod2=1.
Consider (m+n) mod2
We can write this as ((m mod2)+(n mod2)) mod2
Is (1+1) mod2 = 0 is even

Consider (m-n) mod2
We can write this as (1-1) mod2=0
Is even. ✓

Case 3:
Given:

n is an integer
m is an integer
n is even
m is odd

Show:

If m+n is even then m-n is even

Proof:

Since n is even, we know that n mod2=0.
Since m is odd, we know that m mod2=1.
Consider (m+n) mod2
We can write this as ((m mod2)+(n mod2)) mod2
Is (0+1) mod2 = 1 is odd
and the implication will be trivially true.

Case 4:
Given:

n is an integer
m is an integer
n is odd
m is even

Show:

If m+n is even then m-n is even

Proof:

This is essentially similar to case 3.

QED

An alternate proof

Give a proof of the following statement.
For all integer n, m, if m+n is even then m-n is even.

We know that (m+n) mod2 = 0
Add m-n to both sides

(m+n +m–n) mod2 = (m-n) mod2
(2m) mod2 = (m-n) mod2
Replace the 2 by 0 (congruent mod2)
((0)m) mod2 = (m-n) mod2
0 = (m-n) mod2
And therefore, m-n is even.

Problem 9 Prove that $n^5 - n$ is divisible by 5 for all integer n.
We will do a proof by cases
Note: $n^5 - n$ is divisible by 5 iff $\left(n^5 - n\right) \bmod 5 = 0$

And we can freely apply the mod inside to get

$$\left(\left(n \bmod 5\right)^5 - \left(n \bmod 5\right)\right) \bmod 5 = 0$$

Case 1: nmod5 =0

$$\left(n^5 - n\right) \bmod 5 = \left(\left(0\right)^5 - \left(0\right)\right) \bmod 5 = 0 \bmod 5 = 0 \quad ✓$$

Case 2: nmod5 =1

$$\left(n^5 - n\right) \bmod 5 = \left(\left(1\right)^5 - \left(1\right)\right) \bmod 5 = 0 \bmod 5 = 0 \quad ✓$$

Case 3: nmod5 =2

$$\left(n^5 - n\right) \bmod 5 = \left(\left(2\right)^5 - \left(2\right)\right) \bmod 5 = 30 \bmod 5 = 0 \quad ✓$$

Case 4: nmod5 =3

$$\left(n^5 - n\right) \bmod 5 = \left(\left(3\right)^5 - \left(3\right)\right) \bmod 5 = 240 \bmod 5 = 0 \quad ✓$$

Case 5: nmod5 =4

$$\left(n^5 - n\right) \bmod 5 = \left(\left(4\right)^5 - \left(4\right)\right) \bmod 5 = 1020 \bmod 5 = 0 \quad ✓$$

QED

Problem 10 Show that integer division by 3 does not respect the equivalence classes for n mod4.

Note: Multiplication by 3 does respect the equivalence classes for n mod4, because if we pick any two values n and m that are in the same equivalence class, then 3n and 3m are in the same class.

Given: n mod4 = m mod4

Show: (3n)mod4 =(3m)mod4

Proof: (3n)mod4 = (3(nmod4))mod4

= (3(mod4))mod4

=(3m)mod4 ✓

To show that division by 3 does not respect the equivalence classes for mod4, we need to find two values n and m that are in the same equivalence class, but n/3 and m/3 are in different equivalence classes.

n=5 is in [1]

m=1 is in [1]

But n/3 = 1 is in [1]

m/3 = 0 is in [0]