Fall 2016 COT 3100 Section 1 Homework 3 Solutions
Assigned: 9/20/2016
Due: 9/30/2016

1) Prove or disprove: if the quotient (as defined by the division algorithm) when dividing a_1 by b_1 is q_1 and the quotient when dividing a_2 by b_2 is q_2, then the quotient when dividing a_1a_2 by b_1b_2 is q_1q_2.

Solution:

There are many examples that can disprove the statement. Consider following example to disprove it:

$a_1 = 15, b_1 = 4, a_2 = 21, b_2 = 8$

so, $q_1 = \left\lfloor \frac{a_1}{b_1} \right\rfloor = \left\lfloor \frac{15}{4} \right\rfloor = 3$, $q_2 = \left\lfloor \frac{a_2}{b_2} \right\rfloor = \left\lfloor \frac{21}{8} \right\rfloor = 2$

and $\left\lfloor \frac{a_1 a_2}{b_1 b_2} \right\rfloor = \left\lfloor \frac{15 \times 21}{4 \times 8} \right\rfloor = 9$

but $q_1 q_2 = 3 \times 2 = 6$.

So, the statement is not true. The observation here is that a remainder is a leftover less than one "whole part". One way of rewriting the the fraction multiplication shown in the example is $(3 + \frac{3}{4})(2 + \frac{5}{8})$. Notice that product of the quotients of the two separate divisions is simply the first term when you FOIL the expression above. The remainder however plays a role in three of the pieces of FOILing the expression. Since two of those pieces have multiplication with terms greater than one, it's possible that the sum of those pieces is greater than 1.

2) Convert each of the following numbers in base 10 to the designated base.

a) 12345 to base 8

b) 54321 to base 16

c) 9999 to base 7

d) 7364 to base 5

e) 1024 to base 2

Solution

a) 12345 to base 8

dividend	12345	1543	192	24
divisor	8	8	8	8
quotient	1543	192	24	3
remainder	1	7	0	0

So, 12345 in base 10 is equal to 30071 in base 8.

b) 54321 to base 16

dividend	54321	3395	212
divisor	16	16	16
quotient	3395	212	13
remainder	1	3	4

So, 54321 in base 10 is equal to D431 in base 16.

c) 9999 to base 7

dividend	9999	1428	204	29
divisor	7	7	7	7
quotient	1428	204	29	4
remainder	3	0	1	1

So, 9999 in base 10 is equal to: 41103 in base 10.

d) 7364 to base 5

dividend	7364	1472	294	58	11
divisor	5	5	5	5	5
quotient	1472	294	58	11	2
remainder	4	2	4	3	1

So, 7364 in base 10 is equal to 213424 in base 10

e) 1024 to base 2

dividend	1024	512	256	128	64	32	16	8	4	2
divisor	2	2	2	2	2	2	2	2	2	2
quotient	512	256	128	64	32	16	8	4	2	1
remainder	0	0	0	0	0	0	0	0	0	0

So, 1024 in base 10 is equal to: 10000000000 in base 2.

3) Looking at the Fibonacci number recurrence and Euclid's algorithm, explain why the greatest common divisor of two consecutive Fibonacci numbers is always 1. (If you don't know what the Fibonacci numbers are, Google them or look them up in the recommended text.)

Solution

The first 9 number of Fibonacci are as following:

F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9
1	1	2	3	5	8	13	21	34

We want to prove that $\gcd(F_{n+1},F_n)=1$

It is clear that the $\gcd(F_2,F_1)=\gcd(1,1)=1$ (I) and also $F_{n+2}= F_{n+1}+ F_n$

So we can say that:

$\gcd(F_{n+2},F_{n+1}) = \gcd (F_{n+1}+ F_n , F_{n+1})$

then by using the property of gcd it can be concluded that:

$\gcd (F_{n+1}+ F_n , F_{n+1})= \gcd (F_{n+1} , F_n)$ (II)

Since this formula is true for any positive integer $n > 1$, we can repeatedly apply this rule until we show that $\gcd (F_{n+1}+ F_n , F_{n+1}) = \gcd(F_2,F_1) = 1$

4) Determine the greatest common divisor between the following pairs of integers:

a) 123 and 67

b) 871 and 546

c) 609 and 377

d) 399 and 138

Solution

a) 123 and 67
123=67(1) + 57
67 = 57(1)+10
57= 10(5) +7
10 = 7(1) +3
7 = 3(2)+1
3= 1(3) +0
So, gcd(123,67)=1

b) 871 and 546
871 = 546(1)+ 325
546= 325 (1)+ 221
325= 221 (1) + 104
221= 104(2)+ 13
104= 13(8)+0
So, gcd (871,546)=13

c) 609 and 377
609=377(1)+232
377=232(1)+145
232=145(1)+87
145= 87(1)+ 58
87= 58(1)+29
58=29(2)+0
So, gcd(609,377)=29

d) 399 and 138
399=138(2)+123
138=123(1)+15
123=15(8)+3
15=3(5)+0
So, gcd(399,138)=3

5) Prove the following for positive integers, a, b, c and n:

If $an \equiv b(mod c)$, then $\frac{an}{\gcd(a,c)} \equiv \frac{b}{\gcd(a,c)} (mod \frac{c}{\gcd(a,c)})$

Solution

Using the given equation we can convert it to an equality using the definition of mod as follows:

$an = cx + b$, for some integer *x*.
$an - cx = b$

For the purposes of readability, let $d = \gcd(a, c)$. Notice that since $d|a$, $d|c$, and both *n* and *x* are integers, it follows that $d|(an - cx)$. Since the LHS is divisible by d, the RHS must also be, thus $d|b$. Thus, we can divide the equation through by d and each of the expressions $\frac{d}{a}$, $\frac{d}{b}$ and $\frac{d}{c}$ are integers:

$\frac{an-cx}{d} = \frac{b}{d}$
$\frac{a}{d}(n) - \frac{c}{d}(x) = \frac{b}{d}$

$\frac{a}{d}(n) = \frac{c}{d}(x) + \frac{b}{d}$

Finally, we can take this equality and take both sides mod the integer $\frac{c}{d}$, yielding:

$$\frac{an}{d} \equiv \frac{b}{d}(mod\ \frac{c}{d})$$

Substituting back for *d* we get our desired result:

$$\frac{an}{\gcd(a,c)} \equiv \frac{b}{\gcd(a,c)}(mod\frac{c}{\gcd(a,c)})$$

Note: The key here is showing that the three items in question, $\frac{d}{a}$, $\frac{d}{b}$ and $\frac{d}{c}$, are integers.

6) Determine 73^{-1} mod 129 via the Extended Euclidean Algorithm.

Solution

$x \equiv 73^{-1} \bmod 129$

$73x \equiv 1 \bmod 129$

Apply extended Euclidean algorithm:

129=73(1) + 56

73=56(1)+17

56=17(3)+5

17=5(3)+2

5=2(2)+1

Now, we start to substituted from end to start:

a) 1=5-2(2)
b) 2=17-5(3)
   So, 1=5-(17-5(3))(2)
   1=5-17(2)+5(6)
   1=5(7)-17(2)
c) 5=56-17(3)
   So, 1=(56-17(3))(7)-17(2)
   1=56(7)-17(21)-17(2)
   1=56(7)-17(23)
d) 17=73-56
   so, 1=56(7)-(73-56)(23)
   1=56(7)-73(23)+56(23)
   1=56(30)-73(23)

e) 56=129-73
So, 1= (129-73)(30)-73(23)
1=129(30)-73(53)

So, 1= -73(53)

Then $73^{-1} \pmod{129} \equiv -53 \equiv 76$

7) Let a and n be relatively prime positive integers. (Thus, gcd(a, n) = 1.) Consider the set S = $\{ai | i \in Z, 0 \leq i < n\}$. Prove that each value in S is unique mod n. You may use the following theorem in your proof: If x | (yz), and gcd(x, y) = 1, then x | z. (Hint: Use proof by contradiction and assume that two distinct values in the set are equivalent mod n. If two values are equivalent mod n, then their difference is divisible by n.)

Solution

As it is mentioned in the hint we use proof of contradiction to prove this problem. Since it is mentioned in the problem that each value of S is unique mod n, we can assume opposite of this assumption which means for some value is S mod n will be same. Thus we must have:

$ai \equiv aj(mod\ n)$ for $0 < i \neq j < n$

It follows that:

$ai - aj \equiv 9(mod\ n)$
$a(i - j) \equiv 9(mod\ n)$

By using the mod definition we can rewrite above statement as follows n | a(i-j) , since we know from the question that gcd(a,n)=1, then using the theorem given in the problem statement we can deduce that n| (i-j) (I).

Note that i,j < n, so we can say that (i-j)<n (II)

From (I) and (II) we can conclude that i - j = 0, because it is only integer divisible by n in the possible range of values for i - j. So, we can conclude from i-j= 0 that i=j which has contradiction with our initial assumption that i≠j.

Finally, we can say our first assumption was wrong and its contract is true which means that each value of S is unique mod n.

8) Let a be an integer such that $a \equiv 1 \pmod 3$. Prove that $a^3 \equiv 1 \pmod 9$.

Solution

From $a \equiv 1 \pmod 3$ we can say that $a=3n+1$, so we can write a^3 as following:

$a^3 = (3n+1)^3$
$a^3= 27n^3+27n^2+ 9n+1$
$a^3= 9(3n^3+3n^2 + n)+1$

Because n is integer the n^3 and n^2 will be integer too. So, we can rewrite above equation as follows for some integer C:

$a^3= 9(C)+1$

and we can rewrite as :

$a^3 \equiv 1 \pmod 9$

9) Using the result from (a) and the fact that if $x \equiv 1 \pmod m$, $x \equiv 1 \pmod n$, and gcd(m,n) =1, then $x \equiv 1 \bmod (mn)$, prove that

$$\mathbf{666666666667^3 \equiv 1 \pmod{18}.}$$

Solution

As 666666666666 is divisible by 2 and 3, then we can say that $666666666667 \equiv 1 \pmod 2$ and $666666666667 \equiv 1 \pmod 3$. And from previous problem we can say that $666666666667^3 \equiv 1 \pmod 9$. (I)

In addition we know that the odd number cubed is also an odd number, so we can say that: $666666666667^3 \equiv 1 \pmod 2$. (II)

The by knowing that gcd (2,9)=1 and by using the property of modular arithmetic and apply it to (I) and (II) we can say that:

$666666666667^3 \equiv 1 \pmod{2*9}$ so, $666666666667^3 \equiv 1 \pmod{18}$.

10) Recount a paragraph or so about the contributions of Srinivasa Ramanujan, related to computer science. (You may do your research from anywhere, but please do not plagiarize. Write things in your own words.)

Sample Write Up (based on the Wikipedia entry for Ramanujan)

Srinivasa Ramanujan is to mathematics what many consider Mozart to be for music. With minimal formal training in mathematics, Ramanujan derived some of the most complicated known mathematics and even new theorems, completely on his own.

Born in a small village outside of Madras, India in 1887, Ramanujan very quickly showed his affinity for mathematics. By age 11, soon after he had been introduced to formal mathematics in school, he was able to exhaust all of the knowledge of two college boarders who lived at his house. At the age of 16, he obtained a copy of a pure mathematics book and devoured its contents. Using this book as a starting point, he calculated the Euler-Masheroni constant to 15 decimal places. Soon after, Ramanujan attempted to attend college, but due to the fact that all he cared about was mathematics, he earned poor grades in other subjects. After completing school, he spent most of free time doing mathematics, but ultimately had to get a job. He landed a job as a clerk in a revenue department. Upon seeing Ramanujan's notebooks, his boss realized that he didn't deserve such a boring job.

Ramanujan's boss showed the notebooks to other mathematicians in the area. Eventually, these notebooks circulated among a few British mathematicians, several of whom felt that though Ramanujan may have some talent, he lacked formal training and rigor in his proofs. Finally, however, two famous British mathematicians, G. H. Hardy and J. E. Littlewood, felt that Ramanujan's genius deserved to be discovered by others. They offered to have Ramanujan come to England to do mathematical research with them. In 1914, at the age of 27, Ramanujan took a ship from India to England to join Hardy and Littlewood. In working with Hardy and Littlewood, they improved the rigor of the proofs of Ramanujan's results, as often times, Ramanujan relied on his instincts. . In 1918, he was elected a Fellow of the Royal Society, one of the youngest mathematicians to do so and only the second Indian ever, at the time.

Thoughout his life, Ramanujan experienced health problems. Though it was typically thought that he died of tuberculosis, some now believe that he actually died from amoebiasis, a treatable disease that was widespread in Madras at the turn of the 20th century. Ramanujan passed away on April 26, 1920. In six short years of work with Hardy and Littlewood, he produced a great quantity of results. Some of the well-known results he proved dealt with the problem of partitions, the number of ways to divide a postive integer into a set of positive integers. (For example, 4 can be partitioned as follows: 4, 2+2, 1+3, 1+1+2, and 1+1+1+1.), the Bernoulli numbers and coming up with series that can be used to generate many digits of π quickly.