Chris Badolato Ryan Deyoung
Caleb Feliciano

Hw 3

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 $a_1 a_2$ by $b_1 b_2$ is $q_1 q_2$.

$a_1 = b_1 q_1 + r$ $\quad 3 = 2(1) + 1$

$\frac{a_1}{b_1} = q_1 + \frac{r}{b_1}$

$\frac{a_2}{b_2} = q_2 + \frac{r}{b_2}$

$(a_1)(a_2) = (b_1 b_2)(q_1 q_2) + r$

$\frac{(a_1)(a_2)}{(b_1)(b_2)} = (q_1)(q_2) + \frac{r}{b_1 b_2}$

$a_1 = 15 \quad b_1 = 5 \quad q_1 = 3 \quad r = 0$

$a_2 = 20 \quad b_2 = 5 \quad q_2 = 4 \quad r = 0$

$\frac{(15)(20)}{(5)(5)} = (3)(4) + \frac{0}{25} \qquad \frac{300}{25} = 12$ ✓

if our remainer is 0, all values of $(a_1 \cdot a_2)$ divided by $(b_1 \cdot b_2)$ will be equal the values of $(q_1 \cdot q_2)$.

But if our values are so we Disprove

$a_1 = 12 \quad b_1 = 9 \quad q_1 = 1 \quad r_1 = 3$

$a_2 = 3 \quad b_2 = 1 \quad q_2 = 2 \quad r_2 = 1.$

$12 = 9(1) + 3$

$3 = 1(2) + 1$

$\frac{3}{1} = 2 + \frac{1}{1}$ and $\frac{12}{9} = 1 + \frac{3}{9}$ ✓

$\frac{(12)(3)}{(9)(1)} = (1)(2) + \frac{(3)(1)}{9} \qquad \frac{36}{9} = \frac{18}{9} + \frac{3}{9}$

So $\frac{36}{9} \neq \frac{21}{9}$ therefore $\frac{(a_1)(a_2)}{(b_2)(b_1)} \neq (q_1 \cdot q_2)$

Hw 3 Chris Badolato Ryan Deyoung Caleb Feliciano

2 a) 12345 to base 8

$(12345)_{10}$

$12345 = 8 \cdot 1543 + 1$
$1543 = 8 \cdot 192 + 7$
$192 = 8 \cdot 24 + 0$
$24 = 8 \cdot 3 = 0$
$3 = 8 \cdot 0 + 3$

$(30071)_8$

10 = A
11 = B
12 = C
13 = D
14 = E
15 = F
16 = G

B) $(54321)_{10}$ to base 16

$54321 = 16 \cdot 3395 + 1$
$3395 = 16 \cdot 212 + 3$
$212 = 16 \cdot 13 + 4$
$13 = 16 \cdot 0 + 13$

$(D431)_{16}$

C) $(9999)_{10}$ to base 7

$9999 = 7 \cdot 1428 + 3$
$1428 = 7 \cdot 204 + 0$
$204 = 7 \cdot 29 + 1$
$29 = 7 \cdot 4 + 1$
$4 = 7 \cdot 0 + 4$

$(41103)_7$

D) $(7364)_{10}$ to base 5

$7364 = 5 \cdot 1472 + 4$
$1472 = 5 \cdot 294 + 2$
$294 = 5 \cdot 58 + 4$
$58 = 5 \cdot 11 + 3$
$11 = 5 \cdot 2 + 1$
$2 = 5 \cdot 0 + 2$

$(213424)_5$

E) $(1024)_{10}$ to base 2

$1024 = 2 \cdot 512 + 0$
$512 = 2 \cdot 256 + 0$
$256 = 2 \cdot 128 + 0$
$128 = 2 \cdot 64 + 0$
$64 = 2 \cdot 32 + 0$
$32 = 2 \cdot 16 + 0$
$16 = 2 \cdot 8 + 0$
$8 = 2 \cdot 4 + 0$
$4 = 2 \cdot 2 + 0$
$2 = 2 \cdot 1 + 0$
$1 = 2 \cdot 0 + 1$

$(10000000000)_2$

Hw 3 Chris Badolato Ryan Deyoung Caleb Feliciano

(3) $a = bq_0 + r_0$ $\quad F_{n+1} = F_n + F_{n-1}$

$b = r_0 \cdot q_1 + r_1$ $\quad 1, 1, 2, 3, 5, 8, 13, 21$

$r_0 = r_1 \cdot q_2 + r_2$

The greatest common divisor of two consecutive Fibonacci's number is always one because each are mutually Prime.

$gcd(f_2, f_1) = 1$, for $n \geq 2$, we assume $(f_n, f_{n-1}) = 1$

$f_{n+1} = f_n + f_{n-1}$

$a = 3 \quad b = 2 \quad r_0 = 1$

$3 = (1)(2) + 1$.

$2 = (2)(1) + 0$

each f_{n-1} will only divide into each f_n one time with some remainder.

$$\frac{a}{q_0} = b + r_0$$

$$\frac{a}{q_0} - b = r_0.$$

Hw 3 Chris Badolato Ryan Deyoung Caleb Feliciano

4 A) gcd(123, 67)

$123 = 1 \times 67 + 53$

$67 = 1 \times 53 + 14$

$53 = 3 \times 14 + 11$

$14 = 1 \times 11 + 3$

$11 = 3 \times 3 + 2$

$3 = 1 \times 2 + \boxed{1}$

$2 = 2 \times 1 + 0$

1 is our gcd(123, 67)

B] gcd(871, 546)

$871 = 1 \times 546 + 325$

$546 = 1 \times 325 + 221$

$325 = 1 \times 221 + 104$

$221 = 2 \times 104 + \boxed{13}$

$104 = 8 \times 13 + 0$

$\boxed{gcd(123, 67) = 13}$

C) gcd(609, 377)

$609 = 1 \times 377 + 232$

$377 = 1 \times 232 + 145$

$232 = 1 \times 145 + 87$

$145 = 1 \times 87 + 58$

$87 = 1 \times 58 + \boxed{29}$

$58 = 2 \times 29 + 0$

$\boxed{gcd(609, 377) = 29}$

D) gcd(399, 138) = 3

$399 = 2 \times 138 + 123$

$138 = 1 \times 123 + 15$

$123 = 8 \times 15 + \boxed{3}$

$15 = 5 \times 3 + 0$

Hw 3 Chris Badolato Ryan Deyoung Caleb Feliciano

5 prove for positive ints $a, b, c,$ and n

if $an \equiv b \pmod{c}$, then $\frac{an}{gcd(a,c)} \equiv \frac{b}{gcd(a,c)} \pmod{\frac{c}{gcd(a,c)}}$

$10 = 1 \pmod 3$

$b = 1$

$c = 3$

$a = 5$

$n = 2$

$\frac{an}{gcd(5,3)} = \frac{10}{1}$ $\quad \frac{b}{gcd(5,3)} \bmod 2 \frac{c}{gcd(a,c)} = \frac{1}{1} \bmod 2 \frac{3}{1}$

therefore

$10 = 1 \pmod 3 \equiv \frac{1}{1} \bmod 2\ 3 = 10$ ✓

Hw 3 Chris Badolato Ryan Depoong Caleb Feliciano

6 $73^{-1} \bmod 129$

$129 = 73 \times 1 + 56$ (1)

$73 = 56 \times 1 + 17$ (2)

$56 = 17 \times 3 + 3$ (3)

$17 = 3 \times 5 + 2$ (4)

$3 = 2 \times 1 + 1$ (5)

$1 = 3 + 2(-1)$ (6)

$2 = 17 + 3(-5)$ (7)

$3 = 56 + 17(-3)$ (8)

$17 = 73 + 56(-1)$ (9)

$56 = 129 + 73(-1)$ (10)

$3 + (17 + 3(-5))(-1) = 1$

$3 + (17)(-1) + 3(5) = 1$

$17(-1) + 3(6) = 1$

$(-1)(73 + 56(-1)) + (6)(56 + 17(-3)) = 1$

$(-1)73 + 56(1) + 6(56) + 17(-18)) = 1$

$(-1)73 + 56(7) + 17(-18) = 1$

$(-1)73 + (7)(129 + 73(-1)) + (-18)(73 + 56(-1)) = 1$

$(-1)73 + 7(129) + (-7)(73) + (-18)(73) + 18(56) = 1$

$(-26)73 + 7(129) + 18(56) = 1$

$(-26)73 + 7(129) + 18(129 + 73(-1)) = 1$

$(-26)73 + 25(129) + (-18)73 = 1$

$(-44)73 + 25(129) = 1$

$129 - 44 = 85$

$73(85) + 0 = 1 \bmod 129$

$$85 = \frac{1}{73} \bmod 129$$

Hw 3 Chris Badolato

7 a and n are relative prime numbers thus $gcd(a,n) = 1$

prove that each S value is a unique mod n

$S = \{a_i \mid i \in Z,\ 0 \le i \le n$

if $x \mid (yz)$, and $gcd(x,y) = 1$ then $x \mid z$.

if two values are equivalent to mod n then their difference is divisible by n.

$S \equiv 1 \bmod n \equiv \frac{a_{i_1} - a_{i_2}}{n}$ $\quad a_1 \equiv 1 \bmod n$, $a_2 \equiv 1 \bmod n$

$a_{i_1} \equiv a_{i_2} \pmod n$ for $0 \le (a_{i_1})(a_{i_2}) \le n$

$a(i_1 - i_2) \equiv 1 \bmod n$

using mod definition we can rewrite this as

$n \mid a(i_1 - i_2)$ we know $gcd(a,n) =$

we can show that $n \mid (i_1 - i_2)$

therefore $i_2 - i_1 = 0$ and $i_2 = i_1$

But this contradicts that our i values cannot be the same.

finally this proves that S cannot be a unique value of mod n.

Hw 3 Chris Badolato Ryan Deyoung Caleb Feliciano

8 Let a be an int such that $a \equiv 1 \mod 3$
prove $a^3 \equiv 1 \mod 9$

$a = 3c + 1$

$(3c+1)^3 = 1 \mod 9$

$a^3 = (3c)^3 + 3(3c)^2 + 3(3c) + 1$

All terms are multiples of 9 except for 1 so it's Left outside

therefore $a^3 = 9n + 1$

$a^3 = 1 \mod 9$

9 Using results for a in problem 8
also if $x \equiv 1 (\mod m)$, $x \equiv 1 \mod n$ and $\gcd(m,n) = 1$, then $x \equiv 1 \mod (mn)$

$666666666667^3 \equiv 1 (\mod 18)$

odd number cubed is odd.

so $666666666666 + 1$ is a multiple of $3+1$

so x being 666666666667 means that

$x = 1 \mod 3$ 1 being the remainder

as proved in the previous problem, $x^3 = 1 \mod 9$.

So $n = 2$ $m = 1$

$18 = 2 \times 9$ our $\gcd(n,m) = 1$

$x^3 \equiv 1 \mod 18$

Hw3 Chris Badolato

b Srinivasa Ramanujan from Indian was a mathmatician who contributed to analytical theory of numbers. He also work on elliptic functions, continued fractions infinite series and prime numbers which are all important to the mathematics of computer science. Srinivasa searched for patterns in his mathematics, showing relationships between different numbers way ahead of his time, often not having a proof feeling intuitivley that he was correct and often was. His most outstand contribution was his formula for "p(n) or the number of "partitions" of "n". He was a natural genius.