CS 165 Lab Homework

Clark De Leon

Lab Homework:

1) Prove: For $a, b, x \in \mathbb{N}$. If $x \mid a$ and $x \mid b$, then $x \mid (a+b)$

Since $x \mid a$ and $x \mid b$, there are $c, d \in \mathbb{Z}$ such that

$cx = a$, $dx = b$. Then

$$a+b = cx + dx$$

$$a+b = x(c+d)$$

Since $c, d \in \mathbb{Z}$, $c+d \in \mathbb{Z}$.

$\therefore$ $x \mid a+b$ because $x(c+d) = a+b$

2) Prove: For $a, b, n \in \mathbb{N}$, $a \cdot b \pmod{n} \equiv a \pmod{n} \cdot b \pmod{n}$

$a \pmod{n}$ means that $a = nq_1 + r_1$

$b \pmod{n}$ means that $b = nq_2 + r_2$

where r_1, r_2 are remainders in $[0, n)$, q_1 & q_2 are quotients.

So

$a \pmod{n} = r_1$

$b \pmod{n} = r_2$

LHS: $ab \pmod{n}$ =

$$= [(nq_1 + r_1)(nq_2 + r_2)] \pmod{n}$$

$$= [\cancel{nn} q_1 q_2 + \cancel{n} q_1 r_2 + \cancel{n} q_2 r_1 + r_1 r_2] \pmod{n}$$

- Can remove multiples of n because it is mod n

$$= q_1 q_2 + q_1 r_2 + q_2 r_1 + r_1 r_2$$

RHS: $a \pmod{n} \cdot b \pmod{n}$

$$= (\cancel{n} q_1 + r_1) \pmod{n} \cdot (nq_2 + r_2) \pmod{n}$$

- Remove multiples of n

$$= (q_1 + r_1) \pmod{n} \cdot (q_2 + r_2) \pmod{n}$$

$$= q_1 q_2 + q_1 r_2 + q_2 r_1 + r_1 r_2$$

$\therefore$ LHS $\equiv$ RHS

3) <u>Prove:</u> For $p \in \mathbb{N}$ such that $p \geq 5$. If p is prime, then
$p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.

- Every integer can be represented as $6k \pm i$, where k is any integer and i is an integer such that $-1 \leq i \leq 4$
- Now, any integer s that satisfies $6k+0$, $6k+2$, and $6k+4$ is even so s is a multiple of 2 $\Rightarrow$ s is not prime.
- Any integer q that satisfies $6k+3$ is divisible by 3 because the sum of the digits is divisible by $3 \Rightarrow q$ is not prime.
- This leaves us with integers that satisfy $6k \pm 1$. $\Rightarrow$ they are all prime.
- Since all primes are of the form $6k \pm 1$, a prime $p \pmod n$ is congruent to 1 or 5. That is,

$$p = 6k \pm 1 \Rightarrow \begin{array}{l} 6k+1 \equiv 1 \pmod n \\ 6k-1 \equiv 5 \pmod n. \end{array}$$

4) a) $29 \pmod 3 \equiv \underbrace{3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3}_{9 \text{ times}} \cdot 2$

$$\boxed{\equiv 2 \pmod 3}$$

b) $x \in \mathbb{N}$, $51 \equiv 7 \pmod x$

$\boxed{x = 2}$ because $51 \pmod 2 \equiv 1$, $51 = 25(2) + 1$
$7 \pmod 2 \equiv 1$, $7 = 3(2) + 1$

c) $x \in \mathbb{N}$, $4x + 2 \equiv 5 \pmod 7$

	+2	mod 7			
4	6	6	24	26	5
8	10	3	28	30	
12	14	0	32	34	
16	18	4	36	38	
~~18~~	~~20~~	~~6~~	40	42	
20	22	1	44	46	

$x = 6$ because
$4(6) + 2 = 24 + 2$
$= 26 \equiv 5 \pmod 7$

5) a) $243 + 2583 \pmod 3$

$\equiv 3(81) + (3)861 \pmod 3$

$\equiv 3 \cdot 3 \cdot 3 \cdot 3 + 3^2(287) \pmod 3$

$\equiv \cancel{3^4}(1) + \cancel{3^2}(287) \pmod 3$

$\equiv 1 + 287 \pmod 3$

$\equiv 288 \pmod 3$

$\equiv \cancel{3^2}(32) \pmod 3$

$\equiv \boxed{32 \pmod 3}$

b) $248 \cdot 177 \cdot 299 \cdot 492 \cdot 16 \pmod 7$

$\equiv [7^2 + 3] \cdot [7(25) + 2] \cdot [7(42) + 5] \cdot [7(70) + 2] \cdot [7(1) + 2] \pmod 7$

$\equiv 3 \cdot 2 \cdot 5 \cdot 2 \cdot 2 \pmod 7$

$\equiv 120 \pmod 7$

$\equiv 7(17) + 1 \pmod 7$

$\equiv \boxed{1 \pmod 7}$

c) $377^5 \pmod{11}$

$\equiv (11(34) + 3)^5 \pmod{11}$

$\equiv 3^5 \pmod{11}$

$\equiv 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \pmod{11}$

$\equiv 243 \pmod{11}$

$\equiv 11(22) + 1 \pmod{11}$

$\boxed{\equiv 1 \pmod{11}}$

d) $1056^{27} \pmod{13}$

$\equiv (1056)^{12} \cdot (1056)^{12} \cdot 1056^3 \pmod{13}$

$\equiv 1 \cdot 1 \cdot 1056^3 \pmod{13}$

$\equiv 1056^3 \pmod{13}$

$\equiv (1056)(1056)(1056) \pmod{13}$

$\equiv (13(81) + 3)(13(81) + 3)(13(81 + 3) \pmod{13}$

$\equiv 3 \cdot 3 \cdot 3 \equiv 27 \pmod{13}$

$\boxed{\equiv 1 \text{ mod } (13)}$

6) GCD algorithm:

```
[cdele005@hammer ~]$ ./a.out
gcd(48, 84) = 12
gcd(19, 3214) = 1
gcd(51, 36) = 3
gcd(353, 215) = 1
gcd(568, 353) = 1
[cdele005@hammer ~]$
```

7) <u>Prove</u>: There exists exactly one even prime ($x = 2$).

a) Prove $x = 2$ is prime:

- The only nonzero numbers that divides 2 are 2 (itself) and 1.
- Therefore 2 is prime.

b) Prove $x = 2$ is the only even prime:

Assume opposite: there are more even primes $x \geq 2$

Since x is even, there exists a positive integer k such that $x = 2k$.

Hence, $x \mid x$, $2 \mid x$, and $k \mid x$ meaning x has three distinct numbers that divide x.

- Contradiction, because prime numbers only have two two numbers that divide them, itself and 1.

Therefore, 2 is the only even prime.