Michael Chillemi
Hw 6

1. Euler phi function

- $\phi(20)$

$$\phi(20) = \phi(4 \cdot 5)$$
$$= \phi(4)\ \phi(5)$$
$$= \phi(2^2)\ \phi(5)$$
$$= (2^2 - 2^1)\ \phi(5)$$
$$= (4-2)\ \phi(5)$$
$$= 2\phi(5)$$
$$= 2(5-1)$$
$$= (2)(4)$$
$$= 8$$

$\phi(20) = 8$

- $\phi(89)$

$\phi(89) = (89-1) = 88$

- $\phi(1048576)$

8	1048576
8	131072
8	16384
8	2048
8	256
8	32
2	4
2	2
	1

$1048576 = 8^6 \cdot 2^2$

$= 2^3 \cdot 2^3 \cdot 2^3 \cdot 2^3 \cdot 2^3 \cdot 2^3 \cdot 2 \cdot 2$

$= 2^{3+3+3+3+3+3+1+1}$

$= 2^{20}$

$\phi(1048576) = \phi(2^{20})$

$= 2^{20} - 2^{20-1}$

$= 2^{20} - 2^{19}$

$= 2^{10} \cdot 2^{10} - 2^{10} \cdot 2^{9}$

$= 2^{10}(2^{10} - 2^{9})$

$= 1024(1024 - 512)$

$= 1024 \cdot 512$

$= 524288$

$\phi(1048576) = 524288$

- $\phi(p^n)$ for any prime number p
  n is greater than zero

$\phi(p^n) = p^n - p^{n-1}$

6. • $GCD(100, 35)$

$100 = 35 \cdot 2 + 30$

$35 = 30 \cdot 1 + 5$

$30 = 5 \cdot 6 + 0$

$GCD(100, 35) = 5$

- $GCD(256, 35)$

$256 = 35 \cdot 7 + 11$

$35 = 11 \cdot 3 + 2$

$11 = 2 \cdot 5 + 1$

$2 = 1 \cdot 2 + 0$

$GCD(256, 35) = 1$

• $GCD(1111, 111)$

$1111 = 111 \cdot 10 + 1$

$111 = 1 \cdot 111 + 0$

$GCD(1111, 111) = 1$

3. inverse

• $3^{-1} \pmod{256}$

$256 = 3 \cdot 85 + 1$

$3 = 1 \cdot 3 + 0$

$1 = 256 \cdot 1 - 3 \cdot 85$

$1 = 256 \cdot 1 + 9 \cdot (-85)$

$1 = 3 \cdot (-85) \pmod{256}$

$3 \cdot (-85) \equiv 1 \mod 256$

$3^{-1} \equiv 171$

• $7^{-1} \pmod{33}$

$33 = 7 \cdot 4 + 5$

$7 = 5 \cdot 1 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 1 \cdot 2 + 0$

$$1 = 5\cdot 1 - 2\cdot 2$$
$$= 5\cdot 1 - (7\cdot 1 - 5\cdot 1)\cdot 2$$
$$= 5\cdot 3 - 7\cdot 2$$
$$= (33 - 7\cdot 4)\cdot 3 - 7\cdot 2$$

$$1 = 33\cdot 3 - 7\cdot 14$$

$$1 = 33\cdot 3 + 7\cdot 14$$

$$1 \equiv 7\cdot(-14) \mod 33$$
$$7\cdot(-14) \equiv 1 \mod 3$$
$$-14 \equiv 19 \mod 33$$

$$7\cdot 19 \equiv 1 \mod 33$$

$$7^{-1} \equiv 19 \mod 33$$

• $3^{-1} \pmod{79}$

$$79 = 3\cdot 26 + 1$$
$$3 = 1\cdot 3 + 0$$

$$3\cdot 53 \equiv 1 \pmod{79}$$

$$1 = 79\cdot 1 - 3\cdot 26$$

$$\equiv 3^{-1} \equiv 53 \mod 79$$

$$1 \equiv 3\cdot(-26) \pmod{79}$$

$$3\cdot(-26) \equiv 1 \pmod{79}$$

$$-26 \equiv 53 \pmod{79}$$

Extra Credit

Prove $GCD(a+b, b) = GCD(a,b)$

Let $GCD(a,b) = d$ $\forall d \in N$

$a = da_1$ $b = db_1$ $\forall a_1, b_1 \in N$

$gcd(a_1, b_1) = 1$

$a+b = da_1 + db_1$

$a+b = d(a_1+b_1)$ and $b = db_1$

since $gcd(a_1, b_1) = 1$

$gcd(a_1+b_1, b_1) = 1$
Contradiction

multiply d

$gcd(d(a_1+b_1), db_1) = d$
$gcd(a+b, b) = d$

$gcd(a+b, b) = GCD(a,b)$ Proven ✓