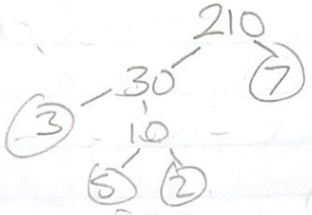
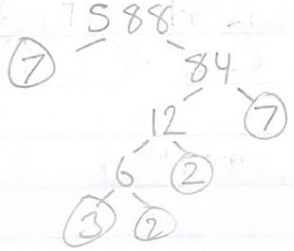
# HW3 - 1.18, 1.20, 1.27

1.18) Compute gcd(210, 588) using Euclid's algorithm & factorization

Factorization




$3 \cdot 5 \cdot 2 \cdot 7 = 210$




$7^2 \cdot 2^2 \cdot 3 = 588$

$3 \cdot 2 \cdot 7 = \boxed{42}$

Euclids Algorithm

Euclid(588, 210)

| a | b | ret |
|---|---|---|
| 588 | 210 | 42 |
| 210 | 168 | 42 |
| 168 | 42 | 42 |
| 42 | 0 | 42 |

Euclid(a, b)
if b=0 then
return a
return Euclid(b, a mod b)

Euclid(588, 210) = $\boxed{42}$

1.20) Find inverse of 20 mod 79, 3 mod 62, 21 mod 91, 5 mod 23

20 mod 79

| a | b | x | y | z | ret1 | ret2 | ret3 |
|---|---|---|---|---|---|---|---|
| 79 | 20 | 1 | -1 | 1 | -1 | 4 | 1 |
| 20 | 19 | 0 | 1 | 1 | 1 | -1 | 1 |
| 19 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | | | | 1 | 0 | 1 |

extended-Euclid(a, b)
if b=0 then
return (1, 0, a)
(x, y, z) = extended-Euclid(b, a mod b)
return (y, x - ⌊a/b⌋y, z)

$1 - \lfloor 79/20 \rfloor \cdot -1 \cdot 4$

$20(4) + 79(-1) = 1$

$ax \equiv 1 \bmod N$ x = inverse

$(\bmod 79)\ 20(4) = 79^{\circ} = 1 \bmod 79$

$20(4) \bmod 79 = 1 \bmod 79$ → 4 is inverse of 20 mod 79

$4 \equiv 20^{-1} \bmod 79$

3 mod 62

| a | b | x | y | z | ret1 | ret2 | ret3 |
|---|---|---|---|---|---|---|---|
| 62 | 3 | 1 | -1 | 1 | -1 | 21 | 1 |
| 3 | 2 | 0 | 1 | 1 | 1 | -1 | 1 |
| 2 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | | | | 1 | 0 | 1 |

$1 - \lfloor 62/3 \rfloor (-1) = 21$
$0 - \lfloor 3/2 \rfloor (1) = -1$
$1 - \lfloor 2/1 \rfloor (0) = 1$

$3(21) + 62(-1) = 1$

$\bmod 62\ (3(21) = 62) = 1 \bmod 62$

$3(21) \bmod 62 \equiv 1 \bmod 62$

$21 \equiv 3^{-1} \bmod 62$

21 is inverse

21 mod 91

| a | b | x | y | z | ret1 | ret2 | ret3 |
|---|---|---|---|---|---|---|---|
| 91 | 21 | 0 | 1 | 7 | 1 | -4 | 7 |
| 21 | 7 | 1 | 0 | 7 | 0 | 1 | 7 |
| 7 | 0 | | | | 1 | 0 | 7 |

4
0 - ⌊91/21⌋(1) = -3
1 - ⌊21/7⌋(0) = 1

$91(1) + 21(-4) = 1$
$\text{mod } 91 \quad 91(1) + 21(-4) = 1 \text{ mod } 91$
$0 + 21(-4) \text{ mod } 91 = 1 \text{ mod } 91$
$-84 \text{ mod } 91 = 1 \text{ mod } 91$
$7 \neq 1 \text{ mod } 91$ ✗

There is no multiplicative inverse

5 mod 23

| a | b | x | y | z | ret1 | ret2 | ret3 |
|---|---|---|---|---|---|---|---|
| 23 | 5 | -1 | 2 | 1 | 2 | -9 | 1 |
| 5 | 3 | 1 | -1 | 1 | -1 | 2 | 1 |
| 3 | 2 | 0 | 1 | 1 | 1 | -1 | 1 |
| 2 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | | | | 1 | 0 | 1 |

-1 - ⌊23/5⌋(2)
1 - ⌊5/3⌋(-1)
0 ⌊3/2⌋(1)
1 - ⌊2/1⌋(0) = 1

$23(2) + 5(-9) = 1$
$\text{mod } 23 \quad 0 + 5(-9) = 1 \text{ mod } 23$
$0 + 5(-9) \text{ mod } 23 = 1 \text{ mod } 23$
$5^{-1} \text{ mod } 23 \equiv -9 \equiv 14$

$23 + (-9) = 14$

14 is the inverse

$(17-1)(23-1) = 352$

1.27) $p=17$, $q=23$, $N=391$, $e=3$, $d=?$ Encryption of $M=41$

$3 \bmod 352$

| a | b | x | v | z | ret1 | ret2 | ret3 |
|---|---|---|---|---|---|---|---|
| 352 | 3 | 0 | 1 | 1 | 1 | -117 | 1 |
| 3 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | // | // | // | 1 | 0 | 1 |

$0 - \lfloor \frac{352}{3} \rfloor (1) = -117$

$1 - \lfloor \frac{3}{1} \rfloor (0) = 1$

$-117 \bmod 352 = 235$

$235(3) \bmod 352 = 1$ ✓

235 is inverse of 3 mod 352

$X^e \bmod N = y$ $\quad X = M = 41$ $e = 3$

| X | y | yodd | z | return |
|---|---|---|---|---|
| 41 | 3 | 1 | 41 | $41 \cdot 41^2 \bmod 391 = 105$ |
| 41 | 1 | 1 | 1 | $41 \cdot 1 \bmod 391 = 41$ |
| 41 | 0 | // | // | 1 |

**M=41 encrypted → y=105**