Leandro Jorge Fernández Vega

n = E-8298

HOMEWORK NUMBER 1

$m = 98$

$k = 75600 \cdot m = 7408800$

Exercise 1.

a) Write the decomposition into primes for the number *k*
b) evaluate the number θ (*k*) of all natural divisors of *k*
c) By using the *Eratosthenes Sieve* determine all the prime numbers not exceeding 100+*m*

A) By Theorem 4.2, $\exists s \in \mathbb{N} / k = \prod_{i=1}^{s} p_i^{\alpha_i}$, p_i prime, $\alpha_i \in \mathbb{Z}$ and the formula is unique.

$k = 7408800$

$7408800 \mid \underline{2}$

$0 \quad 3704400 \mid \underline{2}$

$0 \quad 1852200 \mid \underline{2}$

$0 \quad 926100 \mid \underline{2}$

$0 \quad 463050 \mid \underline{2}$

$0 \quad 231525 \mid \underline{3}$

$0 \quad 77175 \mid \underline{3}$

$0 \quad 25725 \mid \underline{3}$

$0 \quad 8575 \mid \underline{5}$

$0 \quad 1715 \mid \underline{5}$

$0 \quad 343 \mid \underline{7}$

$0 \quad 49 \mid \underline{7}$

$0 \quad 7 \mid \underline{7}$

$0 \quad 1$

$k = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^3$

B) By Corollary 4.2, $\theta(k) = (5+1)(3+1)(2+1)(3+1) = 288$

F.V.

c)

Leandro Jorge Fernández Vega
n = E-8298

$n = 100 + m = 198$

By Example 4.4:

1) we list 2, 3 ... n=198. Let i=1
2) Take a prime Pi and remove all multipliaties.
3) i+=1. Go to 2) until $P_i \geq \sqrt{n} \approx 14'07$
4) the remaining list is the list of primes between 2, n.

2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~,
11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, ~~20~~,
~~21~~, ~~22~~, 23, ~~24~~, ~~25~~, ~~26~~, ~~27~~, ~~28~~, 29, ~~30~~,
31, ~~32~~, ~~33~~, ~~34~~, ~~35~~, ~~36~~, 37, ~~38~~, ~~39~~, ~~40~~,
41, ~~42~~, 43, ~~44~~, ~~45~~, ~~46~~, 47, ~~48~~, ~~49~~, ~~50~~,
~~51~~, ~~52~~, 53, ~~54~~, ~~55~~, ~~56~~, ~~57~~, ~~58~~, 59, ~~60~~,
61, ~~62~~, ~~63~~, ~~64~~, ~~65~~, ~~66~~, 67, ~~68~~, ~~69~~, ~~70~~,
71, ~~72~~, 73, ~~74~~, ~~75~~, ~~76~~, ~~77~~, ~~78~~, 79, ~~80~~,
~~81~~, ~~82~~, 83, ~~84~~, ~~85~~, ~~86~~, ~~87~~, ~~88~~, 89, ~~90~~,
91, ~~92~~, ~~93~~, ~~94~~, ~~95~~, ~~96~~, 97, ~~98~~, ~~99~~, ~~100~~,
101, ~~102~~, 103, ~~104~~, ~~105~~, ~~106~~, 107, ~~108~~, 109, ~~110~~,
~~111~~, ~~112~~, 113, ~~114~~, ~~115~~, ~~116~~, ~~117~~, ~~118~~, ~~119~~, ~~120~~,
~~121~~, ~~122~~, ~~123~~, ~~124~~, ~~125~~, ~~126~~, 127, ~~128~~, ~~129~~, ~~130~~,
131, ~~132~~, ~~133~~, ~~134~~, ~~135~~, ~~136~~, 137, ~~138~~, 139, ~~140~~,
~~141~~, ~~142~~, ~~143~~, ~~144~~, ~~145~~, ~~146~~, ~~147~~, ~~148~~, 149, ~~150~~,
151, ~~152~~, ~~153~~, ~~154~~, ~~155~~, ~~156~~, 157, ~~158~~, ~~159~~, ~~160~~,
~~161~~, ~~162~~, 163, ~~164~~, ~~165~~, ~~166~~, 167, ~~168~~, ~~169~~, ~~170~~,
~~171~~, ~~172~~, 173, ~~174~~, ~~175~~, ~~176~~, ~~177~~, ~~178~~, 179, ~~180~~,
181, ~~182~~, ~~183~~, ~~184~~, ~~185~~, ~~186~~, ~~187~~, ~~188~~, ~~189~~, ~~190~~,
191, ~~192~~, 193, ~~194~~, ~~195~~, ~~196~~, 197, ~~198~~.

As a result, the list of primes we get is:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67,
71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149,
151, 157, 163, 167, 173, 179, 181, 191, 193, 197

F.V.

Leandro Jorge Fernandez Vega

$n = E-8298$

Exercise 2. By using the Euclidean algorithm, evaluate the greatest common divisor of the following pairs of numbers

a) *k* and *10800*
b) *72* and *k*
c) 100+*m* and 101+*m*

A) $7408800 = 10800 \cdot 686 + 0 \Rightarrow \gcd(k, 10800) = 10800$

B) $7408800 = 72 \cdot 102900 + 0 \Rightarrow \gcd(k, 72) = 72$

C)

$100 + m = 198 \qquad 101 + m = 199$

$$\left.\begin{array}{l} 199 = 198 \cdot 1 + 1 \\ 198 = 1 \cdot 198 + 0 \end{array}\right\} \Rightarrow \gcd(198, 199) = 1$$

F.V.

Leandro Jorge Fernández Vega

m = E-8298

Exercise 3.

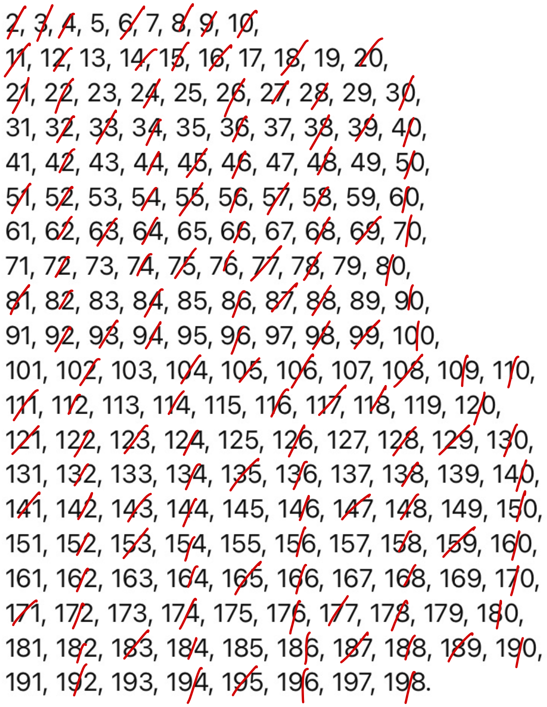
a) List all the invertible elements in Z_{100+m}
b) Determine, by the extended Euclidean Algorithm, the inverse for each of the last three elements of your list from a)
c) Evaluate $(100+m)^{-1}$ in Z_{101+m}

A)

$198 = 2 \cdot 3^2 \cdot 11$

$\mathbb{Z}^*_{198} = \{ x \in \mathbb{Z}_{198} \mid \gcd(x, 198) = 1 \} = \{1, 5, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71, 73, 77, 79, 83, 85, 89, 91, 95, 97, 101, 103, 107, 109, 113, 115, 119, 121, 125, 127, 131, 133, 137, 139, 143, 145, 149, 151, 155, 157, 161, 163, 167, 169, 173, 175, 179, 181, 185, 187, 191, 193, 197\}$

Crossing out all multiplicities of 2, 3, 11 we obtain the elements:



~~2~~, ~~3~~, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~,
~~11~~, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, ~~20~~,
~~21~~, ~~22~~, 23, ~~24~~, 25, ~~26~~, ~~27~~, ~~28~~, 29, ~~30~~,
31, ~~32~~, ~~33~~, ~~34~~, 35, ~~36~~, 37, ~~38~~, ~~39~~, ~~40~~,
41, ~~42~~, 43, ~~44~~, ~~45~~, ~~46~~, 47, ~~48~~, 49, ~~50~~,
~~51~~, ~~52~~, 53, ~~54~~, ~~55~~, ~~56~~, ~~57~~, ~~58~~, 59, ~~60~~,
61, ~~62~~, ~~63~~, ~~64~~, 65, ~~66~~, 67, ~~68~~, ~~69~~, ~~70~~,
71, ~~72~~, 73, ~~74~~, ~~75~~, ~~76~~, ~~77~~, ~~78~~, 79, ~~80~~,
~~81~~, ~~82~~, 83, ~~84~~, 85, ~~86~~, ~~87~~, ~~88~~, 89, ~~90~~,
91, ~~92~~, ~~93~~, ~~94~~, 95, ~~96~~, 97, ~~98~~, ~~99~~, ~~100~~,
101, ~~102~~, 103, ~~104~~, ~~105~~, ~~106~~, 107, ~~108~~, ~~109~~, ~~110~~,
~~111~~, ~~112~~, 113, ~~114~~, 115, ~~116~~, ~~117~~, ~~118~~, 119, ~~120~~,
~~121~~, ~~122~~, ~~123~~, ~~124~~, 125, ~~126~~, 127, ~~128~~, ~~129~~, ~~130~~,
131, ~~132~~, 133, ~~134~~, ~~135~~, ~~136~~, 137, ~~138~~, 139, ~~140~~,
~~141~~, ~~142~~, ~~143~~, ~~144~~, 145, ~~146~~, ~~147~~, ~~148~~, 149, ~~150~~,
151, ~~152~~, ~~153~~, ~~154~~, 155, ~~156~~, 157, ~~158~~, ~~159~~, ~~160~~,
161, ~~162~~, 163, ~~164~~, ~~165~~, ~~166~~, 167, ~~168~~, 169, ~~170~~,
~~171~~, ~~172~~, 173, ~~174~~, 175, ~~176~~, ~~177~~, ~~178~~, 179, ~~180~~,
181, ~~182~~, ~~183~~, ~~184~~, 185, ~~186~~, ~~187~~, ~~188~~, ~~189~~, ~~190~~,
191, ~~192~~, 193, ~~194~~, ~~195~~, ~~196~~, 197, ~~198~~.

F.V.

Leandro Jorge Fernández Vega

$n = E-8298$

B) $\mathbb{Z}_{198}$

- 191^{-1}

$198 = 191 \cdot 1 + 7$ $\quad t_0 = 0,\ t_1 = 1,\ r_0 = 198,\ r_1 = 191$

$191 = 7 \cdot 27 + 2$ $\quad q_1 = 1,\ q_2 = 27,\ q_3 = 3$

$7 = 2 \cdot 3 + 1$

$2 = 1 \cdot 2 + 0$

$t_2 = t_0 - q_1 t_1 \bmod 198 = 0 - 1 \cdot 1 \bmod 198 = -1 \bmod 198$

$t_3 = t_1 - q_2 t_2 \bmod 198 = 1 + 27 \cdot 1 \bmod 198 = 28$

$t_4 = t_2 - q_3 t_3 \bmod 198 = -1 - 3 \cdot 28 \bmod 198 = 113$

$\gcd(r_0, r_1) = 1 \implies$

Due to Euclides Extended Algorithm, $191^{-1} = 113$

- 193^{-1}

$198 = 193 \cdot 1 + 5$ $\quad t_0 = 0,\ t_1 = 1,\ r_0 = 198,\ r_1 = 193$

$193 = 5 \cdot 38 + 3$ $\quad q_1 = 1,\ q_2 = 38,\ q_3 = 1,\ q_4 = 1$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

$t_2 = t_0 - q_1 t_1 \bmod 198 = 0 - 1 \cdot 1 \bmod 198 = -1 \bmod 198$

$t_3 = t_1 - q_2 t_2 \bmod 198 = 1 + 38 \cdot 1 \bmod 198 = 39$

$t_4 = t_2 - q_3 t_3 \bmod 198 = -1 - 1 \cdot 39 \bmod 198 = 158$

$t_5 = t_3 - q_4 t_4 \bmod 198 = 39 - 1 \cdot 158 \bmod 198 = 79$

$\gcd(r_0, r_1) = 1 \implies$

Due to Euclides Extended Algorithm, $193^{-1} = 79$

F.V.

Leandro Jorge Fernández Vega

n = E-8298

- 197^{-1}

$198 = 197 \cdot 1 + 1$ $\quad$ $t_0 = 0,\ t_1 = 1,\ r_0 = 198,\ r_1 = 197$

$197 = 1 \cdot 197 + 0$ $\quad$ $q_1 = 1$

$t_2 = t_0 - q_1 t_1 \bmod 198 = 0 - 1 \cdot 1 \bmod 198 = 197$

$\gcd(r_0, r_1) = 1 \Longrightarrow$

Due to Euclides Extended Algorithm, $197^{-1} = 197$

C) $\mathbb{Z}_{199}$

- 198^{-1}

$199 = 198 \cdot 1 + 1$ $\quad$ $t_0 = 0,\ t_1 = 1,\ r_0 = 199,\ r_1 = 198$

$198 = 1 \cdot 198 + 0$ $\quad$ $q_1 = 1$

$t_2 = t_0 - q_1 t_1 \bmod 198 = 0 - 1 \cdot 1 \bmod 199 = 198$

$\gcd(r_0, r_1) = 1 \Longrightarrow$

Due to Euclides Extended Algorithm, $198^{-1} = 198$

F.V.

Leandro Jorge Fernandez Vega

n = E-8298

Exercise 4. Using the Chinese Remainder Theorem solve the system of congruences:

x= *r₁* mod *4*

x=*r₂* mod *5*

x=*r₃* mod *9*

where

a) *r₁, r₂, r₃* are the remainders of the division of *100+m* by 4, 5, 9, respectively

b) *r₁, r₂, r₃* are the remainders of the division of *100+m* by 2, 3, 8, respectively

$100+m=198$

$\text{mcd}(4,5)=\text{mcd}(4,9)=\text{mcd}(5,9)=1 \Longrightarrow$ It's possible to apply chinese Remainder Theorem.

Let $M=4\cdot5\cdot9=180$, $M_1=\frac{M}{4}=45$, $M_2=\frac{M}{5}=36$, $M_3=\frac{M}{9}=20$

$y_1=M_1^{-1} \bmod 4 = 1^{-1} \bmod 4 = 1$

$y_2=M_2^{-1} \bmod 5 = 1^{-1} \bmod 5 = 1$

$y_3=M_3^{-1} \bmod 9 = 2^{-1} \bmod 9 = 5$

A) $r_1=2,\ r_2=3,\ r_3=0$

$$\left.\begin{array}{l} x=2 \bmod 4 \\ x=3 \bmod 5 \\ x=0 \bmod 9 \end{array}\right\}$$

Due to chinese Remainder theorem, $x=2\cdot45\cdot1+3\cdot36\cdot1+0 \bmod 180=18$

B) $r_1=0,\ r_2=0,\ r_3=6$

$$\left.\begin{array}{l} x=0 \bmod 4 \\ x=0 \bmod 5 \\ x=6 \bmod 9 \end{array}\right\}$$

Due to chinese Remainder theorem, $x=0+0+6\cdot20\cdot5 \bmod 180=60$

F.V.