Exercise 7.

Problem 1.

a) p prime $\varphi(p)$.

$\varphi(p) = |\mathbb{Z}_p^*|$ $\quad \mathbb{Z}_p^* = \{i : \gcd(i,p)=1, i \in \mathbb{Z}_p\}$

$\mathbb{Z}_p = \{0,1,\dots,p-1\}$

$(1,p)=1$

$(2,p)=1$

$\vdots$

$(p-1,p)=1$

$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} \Rightarrow |\mathbb{Z}_p^*| = p-1$

$\Rightarrow \varphi(p) = p-1.$

b) $\varphi(p^k)$ $\quad k \in \mathbb{N}$ $\quad (p^k, n) > 1 \Leftrightarrow$

$p \mid n$

$\mathbb{Z}_{p^k} = \{\overline{0}, 1, \dots, p-1,$

$\overline{p}, p+1, \dots, 2p-1,$

$\overline{2p}, 2p+1, \dots, 3p-1,$

$\vdots$

$\overline{p^k - p}, p^k - p + 1, \dots, p^k - 1\}$

$\varphi(p^k) = p^k - p^{k-1}$

$= p^{k-1}(p-1).$

1.c) $p \neq q$ $\quad \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q)$

$\mathbb{Z}_{pq} = \{0, \dots, pq-1\}$

$(n, pq) > 1 \Rightarrow$ either $p \mid n$ or $q \mid n$

$\mathbb{Z}^*_{pq}$:

number of elements in $\mathbb{Z}_{pq}$ divided by p: q
(m) (m/p)

" " " " " " q : p

$$|\mathbb{Z}^*_{pq}| = \underbrace{|\mathbb{Z}_{pq}|}_{pq} - p - q + 1$$

$\Rightarrow \varphi(pq) = pq - p - q + 1 = (p-1)(q-1)$

$\varphi(p) = p-1 \quad \varphi(q) = q-1$

$$\varphi(pq) = \varphi(p)\,\varphi(q)$$

d) $\varphi(4913) = \varphi(17^3) = 17^2 \times (17-1) = 4624$

$\varphi(899) = \varphi(29 \times 31) = 28 \times 30 = 840.$

$30^2 - 1$

Problem 2. $\varphi(mn) = \varphi(m)\varphi(n)$

$\gcd(m,n) = 1$

Remark: This property implies that if

$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_K^{\alpha_K}$ (Prime factorization)

$\varphi(m) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_K^{\alpha_K})$

$= p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_K^{\alpha_K - 1} (p_1 - 1)(p_2 - 1) \cdots (p_K - 1).$

$\mathbb{Z}_{mn} = \{ 0, 1, 2, \ldots, m-1,$

row $i \longrightarrow$ $m, m+1, \ldots, 2m-1,$

$\vdots$

$m(n-1), m(n-1)+1, \ldots, mn-1 \}$

column K

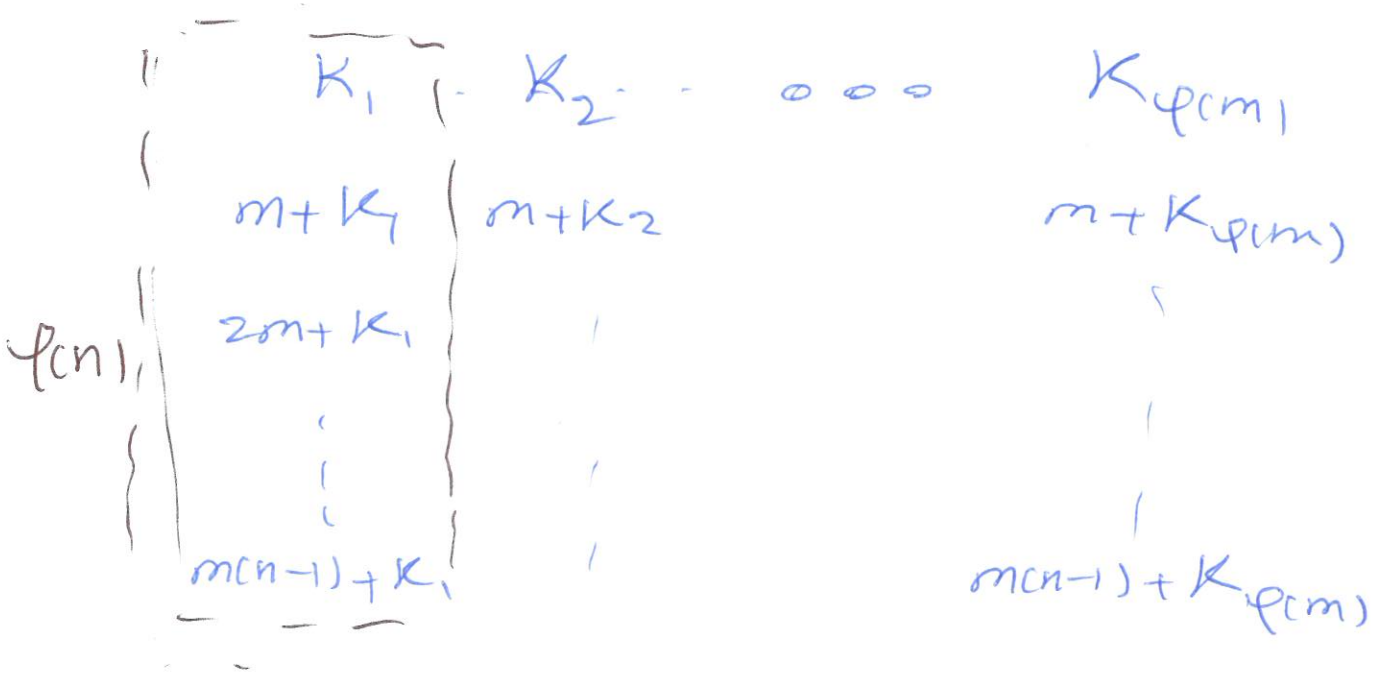
$m(i-1), m(i-1)+1, \ldots, \underbrace{m(i-1)+m-1}_{mi-1}$

$(K, m) > 1 \Rightarrow (mi + K, m) > 1.$

$\left| \{ K \in \mathbb{Z}_m : (K, m) > 1 \} \right| = m - \varphi(m)$

$\mathbb{Z}_m^* = \{ K_1, \ldots, K_{\varphi(m)} \}$

$\varphi(m)$



$$\{K_1, m+K_1, \ldots, m(n-1)+K_1\} = \mathbb{Z}_n \bmod n$$

$(i \neq j)$

if $mi+K_1 = mj+K_1 \bmod n$ then

$$n \mid mi-mj = m(i-j) \Rightarrow n \mid i-j$$

$(i,j) \in \mathbb{Z}_n \Rightarrow n \nmid i-j$ and $(n,m)=1$.

which is a contradiction.

Therefore at each column K_i, there are $\varphi(n)$ elements coprime w.r.t. n.

$$\Rightarrow \quad \varphi(m)\varphi(n) = \varphi(mn).$$

Problem 3. $n \sim \text{Unif}(\{N, \ldots, 2N\})$

$$P(n \text{ is prime}) = \frac{2}{\ln N}$$

MRPT m times

$P(\text{"MRPT returns "prime"} \mid n \text{ is prime}) = 1.$

$P(\text{MRPT returns "comp"} \mid n \text{ is composite}) > \frac{3}{4}$

$$P(\underbrace{n \text{ is composite}}_{A} \mid \underbrace{\text{MRPT returns } m \text{ times "}n \text{ is prime"}}_{B}) =$$

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \qquad f(x) = \frac{a}{x+a}$$

$$P(A) = 1 - \frac{2}{\ln(N)} \qquad P(B|A) \leq \left(\frac{1}{4}\right)^m = \frac{1}{2^{2m}}$$

$$P(B) = P(B|A)P(A) + P(B|A^c)P(A^c)$$

$$\leq \frac{1}{2^{2m}}\left(1 - \frac{2}{\ln N}\right) + \frac{2}{\ln N} \times 1$$

$$P(A|B) \leq \frac{\left(1 - \frac{2}{\ln N}\right) \cdot \frac{1}{2^{2m}}}{\frac{1}{2^{2m}}\left(1 - \frac{2}{\ln N}\right) + \frac{2}{\ln N}}$$

$$= \frac{\ln(N) - 2}{\ln(N) - 2 + 2^{2m+1}}$$

b) $N = 2^{512}$, the above probability $< \frac{1}{1000}$

$m = 2$
0

$$\Phi(-A|B) \leq \frac{\ln(N) - 2}{\ln(N) - 2 + 2^{2m+1}} < \frac{1}{1000}$$

$$\Rightarrow \quad 1000(\ln N - 2) < \ln N - 2 + 2^{2m+1}$$

$$\Rightarrow \quad 2^{2m+1} > 999(\ln N - 2)$$

$$\Rightarrow \quad 2m+1 > \log_2(999(\ln N - 2))$$

$$m > 8.714 \Rightarrow \boxed{m = 9}$$

* $m = \Theta(\log \log N)$.