September 23, 2024

Problem Set 2 Solutions

Exercise 1. Recall that the Euler's totient function $\varphi(n)$ is defined for any $n \in \mathbb{Z}^+$ as the number of positive integers smaller than n, that are coprime to n.

(a) Show that $\varphi(p^k) = p^k - p^{k-1}$, where p is a prime and $k \in \mathbb{Z}^+$.

(b) Show that $\varphi(p_1p_2) = (p_1 - 1)(p_2 - 1)$, where $p_1 \neq p_2$ are two distinct primes.

(c) Compute $\varphi(n)$ for all natural $n \leq 20$.

(d) Assuming that for any $a, b \in \mathbb{Z}^+$ such that $\gcd(a, b) = 1$ $\varphi(ab) = \varphi(a)\varphi(b)$ (we will prove this later), derive a formula for $\varphi(n)$ in terms of the prime factorization of n.

(e)* Let $m_n = p_1p_2 \dots p_n$ denote a product of the first n primes. Show that

$$\lim_{n\to\infty} \frac{\varphi(m_n)}{m_n} = 0.$$

Hint: Use the fact that $\displaystyle\sum_{i=1}^{\infty} \frac{1}{p_i}$ is divergent.

Solution 1. (a) Since p is a prime, the only numbers that have nontrivial common divisors with p^k are the multiples of p. There are $p^k - 1$ total positive integers smaller than p^k, and $(p^{k-1} - 1)$ of them are multiples of p. Therefore, $\varphi(p^k) = p^k - 1 - (p^{k-1} - 1) = p^k - p^{k-1}$. In particular $\varphi(p) = p - 1$.

(b) Let us count the number of positive integers $< p_1p_2$ that have nontrivial common divisors with p_1p_2. We have $p_1p_2 - 1$ positive integers smaller than p_1p_2. Out of these, $(p_2 - 1)$ are multiples of p_1 and $(p_1 - 1)$ are multiples of p_2. Since p_1 and p_2 are distinct primes, no other number $< p_1p_2$ can have a nontrivial common divisor with p_1 or p_2. So we have:

$$\varphi(p_1p_2) = p_1p_2 - 1 - (p_2 - 1) - (p_1 - 1) = p_1p_2 - p_2 - p_1 + 1 = (p_1 - 1)(p_2 - 1).$$

(c)

$$\varphi(1) = 1, \quad \varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2, \quad \varphi(5) = 4, \quad \varphi(6) = 2, \quad \varphi(7) = 6,$$
$$\varphi(8) = 4, \quad \varphi(9) = 6, \quad \varphi(10) = 4, \quad \varphi(11) = 10, \quad \varphi(12) = 4, \quad \varphi(13) = 12, \quad \varphi(14) = 6,$$
$$\varphi(15) = 8, \quad \varphi(16) = 8, \quad \varphi(17) = 16, \quad \varphi(18) = 6, \quad \varphi(19) = 18, \quad \varphi(20) = 8.$$

(d) Let $n = p_1^{a_1} p_2^{a_2} \dots p_m^{a^m}$ be the prime factorization of n. Since the primes $p_i \neq p_j$, we have

$$\varphi(n) = \prod_{i=1}^{m} \varphi(p_i^{a_i}) = \prod_{i=1}^{m} p^{a_i} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{m} p_i^{a_i} \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right).$$

(e) By the formula above we have $\frac{\varphi(m_n)}{m_n} = \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right)$. Consider the limit of the inverse expression:

$$\lim_{n\to\infty} \frac{m_n}{\varphi(m_n)} = \lim_{n\to\infty} \prod_{i=1}^{n} \frac{1}{1 - \frac{1}{p_i}} = \lim_{n\to\infty} \prod_{i=1}^{n} \sum_{k=0}^{\infty} \frac{1}{p_i^k} \geq$$

$$\geq \lim_{n\to\infty} \prod_{i=1}^{n} \left(1 + \frac{1}{p_i}\right) \geq \lim_{n\to\infty} \left(1 + \sum_{i=1}^{n} \frac{1}{p_i}\right) \geq \sum_{i=1}^{\infty} \frac{1}{p_i} = \infty.$$

Here we use that $\displaystyle\sum_{i=1}^{\infty} \frac{1}{p_i}$ is divergent. Since the quantity $\frac{m_n}{\varphi(m_n)}$ grows to infinity as $n \to \infty$, we can conclude that the inverse limit is zero:

$$\lim_{n\to\infty} \frac{\varphi(m_n)}{m_n} = 0.$$

Exercise 2. Recall that for an RSA encryption we need a number N that is a product of two large distinct primes and an encryption key e such that $\gcd(e, \varphi(N)) = 1$, where $\varphi(N)$ is the Euler totient function of N. Any number M in the set $\{1, 2, \dots N\}$ can be encoded by computing $C = M^e \ (\text{mod} N)$. The decryption key consists of a number d such that $ed \equiv 1 \ (\text{mod} \varphi(N))$. We have proved in class that if we know d, we can decode the original message M as $M = C^d \ (\text{mod} N)$. For this exercise suppose that $N = 527$ and $e = 17$.

(a) Encode the message $M = 113$.

(b) Encode the message $M = 500$.

(c) This RSA example has weak security because the number N is small. Break the RSA by factoring N and finding $\varphi(N)$ and d.

(d) Using the value of d found above, decode the message $C = 3$.

(e) Check that for C found in (a), you have $C^d \equiv 113 \ (\text{mod}) \ 527$, so that indeed you can recover the original message.

Solution 2. (a) We need to compute $C = M^e \ (\text{mod} N) = 113^{17} \ (\text{mod} \ 527)$. The number 113^{17} is too large to handle by a calculator, but we can use the properties of congruences to simplify the computation. We find $113^2 = 12769 \equiv 121 \ (\text{mod}) \ 527$. Note that $e = 2^4 + 1$. The number e is often chosen in a form that allows to speed up the computation. Then we repeat the same idea to compute

$$113^{17} \equiv (((113^2)^2)^2)^2 \cdot 113 \ (\text{mod}) \ 527 \equiv ((121^2)^2)^2 \cdot 113 \ (\text{mod}) \ 527 \equiv (412^2)^2 \cdot 113 \ (\text{mod}) \ 527 \equiv$$

$$\equiv 50^2 \cdot 113 \ (\text{mod}) \ 527 \equiv 28 \ (\text{mod}) \ 527.$$

So $C = 28$.

(b) Similarly to the previous exercise we need to compute $C = M^e \ (\text{mod}) \ N = 500^{17} \ (\text{mod}) \ 527$. Here we can use the prime decomposition of $M = 500 = 5^3 \cdot 2^2$ to simplify further the computations. We have:

$$(5^3)^{17} = (5^4)^{12} \cdot 5^3 = 625^{12} \cdot 125 \equiv (((98)^3)^2)^2 \cdot 125 \ (\text{mod}) \ 527 \equiv (497^2)^2 \cdot 125 \ (\text{mod}) \ 527 \equiv$$

$$\equiv 373^2 \cdot 125 \ (\text{mod}) \ 527 \equiv 125 \ (\text{mod}) \ 527.$$

$$(2^2)^{17} = (2^{10})^3 \cdot 2^4 \equiv 1024^3 \cdot 16 \ (\text{mod}) \ 527 \equiv (-30)^3 \cdot 16 \ (\text{mod}) \ 527 \equiv -387 \ (\text{mod}) \ 527 \equiv 140 \ (\text{mod}) \ 527.$$

Finally we have

$$500^9 \ (\text{mod}) \ 527 \equiv 125 \cdot 140 \ (\text{mod}) \ 527 \equiv 109 \ (\text{mod}) \ 527.$$

So $C = 109$.

(c) Since we know that N is a product of exactly two distinct primes, we need to check the divisibility of N by the primes up to $\sqrt{N}$, in this case $\sqrt{527} \cong 22.9$. Dividing by the primes up to 19 gives immediately $527 = 17 \cdot 31$. Then we can compute the Euler totient function of N: $\varphi(p \cdot q) = (p-1)(q-1)$ for two distinct primes p and q, so we have $\varphi(527) = 16 \cdot 30 = 480$. We have $\gcd(17, 480) = 1$, therefore we can find $d \in \mathbb{N}$ such that $ed + k\varphi(N) = 1$ for some $k \in \mathbb{Z}$. Using the Euclid's algorithm for 480 and 17 we easily find

$$1 = 113 \cdot 17 - 4 \cdot 480.$$

Therefore, $d = 113$.

(d) Now to decode the message we need to compute $M = C^d \ (\text{mod}) \ 527 = 3^{113} \ (\text{mod}) \ 527$. We can easily find $3^{10} \equiv 25 \ (\text{mod}) \ 527$, and then

$$3^{113} = (3^{10})^{11} \cdot 27 \equiv 25^{11} \cdot 27 \ (\text{mod}) \ 527 \equiv (25^5)^2 \cdot 25 \cdot 27 \ (\text{mod}) \ 527 \equiv 315^2 \cdot 25 \cdot 27 \ (\text{mod}) \ 527 \equiv 445 \ (\text{mod}) \ 527.$$

So the message was $M = 445$.

(e) Here we have to check $28^{113} \equiv 113 \ (\text{mod}) \ 527$. This is a direct computation. To check your computations here is an online power congruences calculator: `https://www.omnicalculator.com/math/power-modulo`.

Exercise 3. Show that the set B of all matrices of the form

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}, \quad a, b \in \mathbb{R}, \;\; a \neq 0$$

is a group with respect to the matrix multiplication.
Consider the following subsets in B:

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \right\}_{a \neq 0} \quad U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\}_{b \in \mathbb{R}} \quad K = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \right\}_{a > 0, b \geq 0}$$

Which of D, U, K are subgroups of B?

Solution 3. We can check directly that the set B is a group by finding the inverse and the product of two arbitrary matrices in B and observing that the resulting matrix has the same form.

The set K is not a subgroup, because the inverse to the element

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$$

is the element

$$\begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix},$$

which is not in K, because $-b \leq 0$.

The sets D and U are both subgroups in B.

Exercise 4. Consider the transformations in $\mathbb{R}^2$ given by the matrices

$$S_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad S_1 = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

Check that $S_0^2 = 1$ and $S_1^2 = 1$. Let G be the group generated by S_0 and S_1. Find all elements of G and write down a multiplication table between them.

Hint: Since $S_0^2 = S_1^2 = 1$, the only nontrivial elements in G are the products where S_0 and S_1 alternate. Find all distinct elements of this form and determine their products.

Solution 4. The relations $S_0^2 = 1$, $S_1^2 = 1$ follow by direct computation. Since S_0 and S_1 are generators, we have that S_0S_1 and S_1S_0 are elements of the group. They are distinct:

$$S_0S_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix},$$

$$S_1S_0 = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

However, the triple products are the same: $S_0S_1S_0 = S_1S_0S_1$:

$$S_0S_1S_0 = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} = S_1S_0S_1.$$

Using this and $S_0^2 = 1, S_1^2 = 1$, we find $S_0S_1S_0S_1 = S_1S_0$, $S_0S_1S_0S_1S_0 = S_1$, and $S_1S_0S_1S_0 = S_0S_1$, $S_1S_0S_1S_0S_1 = S_0$.
We have $(S_0S_1)^3 = (S_1S_0)^3 = 1$. Therefore there the group generated by S_0 and S_1 has 6 elements: $\{1, S_0, S_1, S_0S_1, S_1S_0, S_0S_1S_0\}$.
It can be written in terms of generators and relations as follows:

$$G = \langle S_0, S_1 \mid S_0^2 = 1, S_1^2 = 1, S_0S_1S_0 = S_1S_0S_1 \rangle.$$

The multiplication table has the form:

	1	S_0	S_1	S_0S_1	S_1S_0	$S_0S_1S_0$
1	1	S_0	S_1	S_0S_1	S_1S_0	$S_0S_1S_0$
S_0	S_0	1	S_0S_1	S_1	$S_0S_1S_0$	S_1S_0
S_1	S_1	S_1S_0	1	$S_1S_0S_1$	S_0	S_0S_1
S_0S_1	S_0S_1	$S_0S_1S_0$	S_0	S_1S_0	1	S_1
S_1S_0	S_1S_0	S_1	$S_1S_0S_1$	1	S_0S_1	S_0
$S_0S_1S_0$	$S_0S_1S_0$	S_0S_1	S_1S_0	S_0	S_1	1

The element in the left column stands on the left in the product.