BTI4202 - Exercise Sheet 2

Jan Fuhrer, Andy Bigler, Joel Häberli

April 19, 2023

Contents

1 Number of primes

The function $\pi(n)$ calculates the number of primes contained in the intervall $\{1, .., n\}$. One Approximation is given wit $\pi(n) = \frac{n}{ln(n)}$

1. Estimate number of 4-digit primes in $[1000, 9999]$:

$$\pi(9999) - \pi(1000) = \frac{9999}{ln(9999)} - \frac{1000}{ln(1000)} \approx 941$$

2. Probability, that a random 4-digit integer in $[1000, 9999]$ is prime:

$$\frac{941}{8999} \approx 10\%$$

2 Eulers Totient Function

Task Compute values of Eulers Totient function $\phi(n)$ for values $n \in [11, 20]$ and $n = 41140$

Process

1. Find prime decomposition for each n.
2. Use best fitting **method** of:
   (a) $\phi(n) = n \cdot \Pi_{i=1}^{k}(1 - \frac{1}{p_i})$, for n an arbitrary decomposition in primes.
   (b) $\phi(p) = p - 1$, for p prim $(n = p)$.
   (c) $\phi(pq) = (p - 1)(q - 1)$, for p, q prim $(n = p \cdot q)$.

Results

n	prime decomposition	$\phi(n)$	**method**
11	11	$\phi(11) = 11 - 1 = 10$	b
12	$2^2 \cdot 3$	$\phi(12) = 12 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3}) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12 \cdot \frac{1}{3} = 4$	a
13	13	$\phi(13) = 13 - 1 = 12$	b
14	$2 \cdot 7$	$\phi(14) = 1 \cdot 6 = 6$	c
15	$3 \cdot 5$	$\phi(15) = 2 \cdot 4 = 8$	c
16	2^4	$\phi(16) = 16 \cdot (1 - \frac{1}{2}) = 16 \cdot \frac{1}{2} = 8$	a
17	17	$\phi(17) = 17 - 1 = 16$	b
18	$2 \cdot 3^2$	$\phi(18) = 18 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3}) = 18 \cdot \frac{1}{2} \cdot \frac{2}{3} = 18 \cdot \frac{1}{3} = 6$	a
19	19	$\phi(19) = 19 - 1 = 18$	b
20	$2^2 \cdot 5$	$\phi(20) = 20 \cdot (1 - \frac{1}{2})(1 - \frac{1}{5}) = 20 \cdot \frac{1}{2} \cdot \frac{4}{5} = 20 \cdot \frac{2}{5} = 8$	a

Task $\phi(41140)$ Prime decomposition: $2^2 \cdot 5 \cdot 11^2 \cdot 17$

$$\phi(41140) =$$

$$41140 \cdot (1 - \frac{1}{2})(1 - \frac{1}{5})(1 - \frac{1}{11})(1 - \frac{1}{17}) =$$

$$41140 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{10}{11} \cdot \frac{16}{17} =$$

$$41140 \cdot \frac{640}{1870} =$$

$$14080$$

3 Euler's Theorem

Theorem 1 (Euler's Theorem) *Let a and n be two positive integers $a \in \{1, .., n-1\}$ and $gcd(a, n) = 1$, then*

$$1 \equiv a^{\phi(n)} mod\ n$$

Check 1 (n = 9) $\phi(9) = 9 \cdot \frac{2}{3} = 6$

a	$gcd(a, 9) = 1$	$a^{\phi(9)} mod\ 9$
1	*true*	*1*
2	*true*	*1*
3	*false*	*0*
4	*true*	*1*
5	*true*	*1*
6	*false*	*0*
7	*true*	*1*
8	*true*	*1*

Check 2 (n = 10) $\phi(10) = 10 \cdot \frac{2}{5} = 4$

a	$gcd(a, 10) = 1$	$a^{\phi(10)} mod\ 10$
1	*true*	*1*
2	*false*	*0*
3	*true*	*1*
4	*false*	*0*
5	*false*	*0*
6	*false*	*0*
7	*true*	*1*
8	*false*	*0*
9	*true*	*1*

Corollary 1 *As we recognize the check $1 \equiv a^{\phi(n)} mod\ n$ is successful for each a if $gcd(a, n) = 1$ for the given $n \in \{9, 10\}$.*

4 Primitive Root Modulo n

Definition 1 (Primitive Root Modulo n) *Let a, k, g, n be positive integers with $a, k \in \{1, .., n\}$ and $g > 0$. g is called a primitive root modulo n if for each a there exists any k such that $a = g^k \ mod \ n$.*

Check 3 (Primitive Roots modulo 7) *Primitive roots modulo 7:* $(3, 5)$

Task (3)

- $(3^0 \ mod \ 7 = 1)$
- $(3^1 \ mod \ 7 = 3)$
- $(3^2 \ mod \ 7 = 2)$
- $(3^3 \ mod \ 7 = 6)$
- $(3^4 \ mod \ 7 = 4)$
- $(3^5 \ mod \ 7 = 5)$

Task (5)

- $(5^0 \ mod \ 7 = 1)$
- $(5^1 \ mod \ 7 = 5)$
- $(5^2 \ mod \ 7 = 4)$
- $(5^3 \ mod \ 7 = 6)$
- $(5^4 \ mod \ 7 = 2)$
- $(5^5 \ mod \ 7 = 3)$

Check 4 (Primitive Roots modulo 8) *No primitive roots.*

5 Multiplicative Groups over Integers modulo n

Task ($\mathbb{Z}_6^*$) prime factorisation: $2 \cdot 3$

$$\phi(6) = 2$$

$$\mathbb{Z}_6^* = \{1, 5\}$$

Task ($\mathbb{Z}_7^*$) 7 is prime, so

$$\phi(7) = 6$$

$$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$

Task ($\mathbb{Z}_8^*$) prime factorisation: 2^3

$$\phi(8) = 4$$

$$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$$

Task ($\mathbb{Z}_9^*$) prime factorisation: 3^2

$$\phi(9) = 6$$

$$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$$

Task ($\mathbb{Z}_{10}^*$) prime factorisation: $2 \cdot 5$

$$\phi(10) = 1 \cdot 4 = 4$$

$$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$$

Task ($\mathbb{Z}_{12}^*$) prime factorisation: $2^2 \cdot 3$

$$\phi(12) = 4$$

$$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$$

Task ($\mathbb{Z}_{13}^*$) 13 is prime, so

$$\phi(13) = 12$$

$$\mathbb{Z}_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

Task ($\mathbb{Z}_{14}^*$) prime factorisation: $2 \cdot 7$

$$\phi(14) = 1 \cdot 6 = 6$$

$$\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$$

Task Multiplication table for $\mathbb{Z}_9^*$:

9	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Pairs of inverse elements:

- $(1, 1)$

- $(2, 5)$
- $(4, 7)$
- $(5, 2)$
- $(7, 4)$
- $(8, 8)$

6 Multiplicative Subgroups of Integers modulo 9

Task Determine all the subgroups of $(\mathbb{Z}_9^*, x_n, ^{-1}, 1)$ and check if Lagrange's theorem holds. Determine the generators of $\mathbb{Z}_9^*$.

Process Divider from $ord(\mathbb{Z}_9^*) = 6$ are $\{1, 2, 3\}$. Subgroups of $\mathbb{Z}_9^*$:

- $\langle 1 \rangle = 1^1 = 1,\ 1^2 = 1,\ ... = \mathbb{G}_1 = \{1\}$
- $\langle 2 \rangle = 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 7,\ 2^5 = 5,\ 2^6 = 1 = \mathbb{Z}_9^*$
- $\langle 4 \rangle = 4^1 = 4,\ 4^2 = 7,\ 4^3 = 1,\ ... = \mathbb{G}_3 = \{1, 4, 7\}$
- $\langle 5 \rangle = 5^1 = 5,\ 5^2 = 7,\ 5^3 = 8,\ 5^4 = 4,\ 5^5 = 2,\ 5^6 = 1 = \mathbb{Z}_9^*$
- $\langle 7 \rangle = 7^1 = 7,\ 7^2 = 4,\ 7^3 = 1,\ ... = \mathbb{G}_3 = \{1, 4, 7\}$
- $\langle 8 \rangle = 8^1 = 8,\ 8^2 = 1,\ ... = \mathbb{G}_2 = \{1, 8\}$

Final list:

- $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\} = \mathbb{G}_6$
- $\mathbb{G}_1 = \{1\}$
- $\mathbb{G}_2 = \{1, 8\}$
- $\mathbb{G}_3 = \{1, 4, 7\}$

9	1
1	1

9	1	8
1	1	8
8	8	1

9	1	4	7
1	1	4	7
4	4	7	1
7	7	1	4

Task Determine the generators of $\mathbb{Z}_9^*$.

Process Create exponential table for $\mathbb{Z}_9^*$:

9	1	2	3	4	5	6	...
1	1	1	1	1	1	1	...
2	2	4	8	7	5	1	...
4	4	7	1	4	7	1	...
5	5	7	8	4	2	1	...
7	7	4	1	7	4	1	...
8	8	1	8	1	8	1	...

Result A generator of $\mathbb{Z}_9^*$ is given for a group element x if $ord(x) = ord(\mathbb{Z}_9^*)$.

x	1	2	4	5	7	8
$ord(x)$	1	6	3	6	3	2

So, the generators of $\mathbb{Z}_9^*$ are $\{2, 5\}$.