SOLUTIONS FOR THE 11$^{\text{TH}}$ INTERNATIONAL TOURNAMENT OF YOUNG MATHEMATICIANS

Team Bulgaria

Problem 9: Maximal Order of Residues

Author: Ivan Durev, Plamen Ivanov

Abstract

We have explored the properties of primitive roots of a number, which helped us solve almost all of item 1. We also did research on the definition of arithmetic operations over Gaussian numbers and on primitive roots in Gaussian numbers (item 2) which empowered us to calculate some of the values. We have completely solved items 1a, 1b and 1c, 1d and partially 1e. Calculations for item 2 are given. We have proved useful foundation theorems regarding the topic.

Maximal Order of Residues

Definition 1. Let a and n be two coprime numbers and $r \in \mathbb{Z}^+$ is the least number, for which $a^r \equiv 1 \pmod{n}$

Theorem 1. Let r be the order of a modulo n ($gcd(a; n) = 1$). Then $a^l \equiv 1 \pmod{n} \iff r \mid l$

Proof of the " $\implies$ " direction. Let us suppose the opposite - that $r \nmid l$. Let $l = kr + q$, $k \in \mathbb{Z}$, $k \geq 0$ and $q \in \{1, 2, \ldots, r-1\}$

$$\begin{aligned} & a^r \equiv 1 \pmod{n} \\ & a^q r \equiv 1 \pmod{n} \\ & a^q r + q \equiv 1 \pmod{n} \\ & a^q \equiv 1 \pmod{n} \text{ But } q < r \\ \implies & \text{Contradiction with the definition of the order of a number.} \quad \blacksquare \end{aligned}$$

Proof of the "$\impliedby$" direction.

$$\begin{aligned} & a^r \equiv 1 \pmod{n} \\ & \text{As } \frac{l}{r} \in \mathbb{Z}^+ \implies (a^r)^{\frac{l}{r}} \equiv 1^{\frac{l}{r}} \pmod{n} \\ \implies & a^l \equiv 1 \pmod{n} \qquad \blacksquare \end{aligned}$$

Theorem 2. Let r be the order of a modulo n ($gcd(a; n) = 1$) and $k \in \mathbb{Z}^+$. Then, the order of a^k is $\dfrac{r}{gcd(k; r)}$

Proof. Let $gcd(k; r) = d$ and $k = dk_1$, $r = dr_1 \implies gcd(k_1; r_1) = 1$

Let the order of a^k modulo n be t.

$$\begin{aligned} (a^k)^{r_1} = a^{dk_1r_1} = (a^r)^{k_1} \equiv 1 \pmod{n} \\ \implies \text{From } \textbf{Theorem 1.} \implies t \mid r_1 \\ (a^k)^t = a^{kt} \equiv 1 \pmod{n} \implies r \mid kt \\ \implies r_1 \mid k_1 t, \text{ but } gcd(r_1; k_1) = 1 \implies r_1 \mid t \\ \text{From the two conclusions above} \implies t = r_1 = \frac{r}{gcd(r; k)} \quad \blacksquare \end{aligned}$$

Theorem 3. Let r be the order of a modulo n ($gcd(a; n) = 1$) and s be the order of b modulo n. Then, the following are true:

(1) If $gcd(r; s) = 1$, then the order of ab modulo n is rs.

(2) $\exists c$ such that its order modulo n is $lcm[r; s]$

Proof of (1). Let t be the order of ab modulo n.

$(ab)^{rs} = a^{rs}b^{rs} \equiv 1 \pmod{n}$

$\implies$ From **Theorem 1.** $t \mid rs$

$a^t b^t = (ab)^t \equiv 1 \pmod{n} \implies (ab)^{ts} \equiv 1 \pmod{n}$

Because $b^{ts} \equiv 1 \pmod{n} \implies a^{ts} \equiv 1 \pmod{n} \implies r \mid ts$

But $gcd(r; s) = 1 \implies r \mid t$

Analogically, $s \mid t$, but $gcd(r; s) = 1 \implies rs \mid t$

From the two conclusions above $\implies t = rs$ ■

Proof of (2). Let $r = \prod_{i=1}^{m} p_i^{k_i}$ and $s = \prod_{i=1}^{m} p_i^{l_i}$, where p_i are distinct primes and $k_i \in \mathbb{Z}$, $l_i \in \mathbb{Z}$ and $k_i \geq 0, l_i \geq 0$ for $i = \{1, 2, \ldots, m\}$.
$lcm[r; s] = \prod_{i=1}^{m} p_i^{u_i}$, where $u_i = max(k_i; l_i)$
There exists a number c_1 with order $p_1^{u_1}$ modulo n because if the number $u_1 = k_1$ (W.L.G.), then from **Theorem 2.** the number $a^{r/p_1^{u_1}}$ will be of order $p_1^{u_1}$.
Continuing the same way we can state that there exists a number c_i of order $p_i^{u_i}$ modulo n for every $i \in \{1, 2, \ldots, m\}$.
As the numbers $p_1^{u_1}, p_2^{u_2}, \ldots, p_m^{u_m}$ are pairwise coprime, then with multiple applications of **Theorem 3(1).** we get that the number $c = \prod_{i=1}^{m} c_i$ is of order $lcm[r; s]$ ■

Item 1a. *Solution.* According to **Euler's theorem**, $a^{\phi(n)} \equiv 1 \pmod{n}$.
$\implies$ Because the order is the minimal power so that a to that power has a remainder 1 modulo n, the order is less or equal to $\phi(n)$. Therefore, $f(n)$ is finite.

Item 1b. *Solution.* Let's consider n to be the modulus for which we are calculating $f(n)$ and $g(n)$. Then, after calculating the orders of all coprime numbers to n less than n:

$n = 2$	$f(2) = 1$	$g(2) = 1$	(1)
$n = 3$	$f(3) = 2$	$g(3) = 1$	(2)
$n = 4$	$f(4) = 2$	$g(4) = 1$	(3)
$n = 5$	$f(5) = 4$	$g(5) = 2$	$(2, 3)$
$n = 6$	$f(6) = 2$	$g(6) = 1$	(5)
$n = 7$	$f(7) = 6$	$g(7) = 2$	$(3, 5)$
$n = 8$	$f(8) = 2$	$g(8) = 3$	$(3, 5, 7)$
$n = 9$	$f(9) = 6$	$g(9) = 2$	$(2, 5)$
$n = 10$	$f(10) = 4$	$g(10) = 2$	$(3, 7)$

■

Definition 2. If $gcd(a;n)=1$ and $\phi(n)$ is the order of a modulo n, then we call a a *primitive root* modulo n.

Theorem 4. For every prime number p there exists at least one primitive root.
Proof. Let $P=\{1,2,\ldots,p-1\}$ be the set of remainders modulo p. Let $a\in P$ be the number with greatest order modulo p. We will denote this number by r. From **Item 1a.** $\implies r\le\phi(p)=p-1$. For every number $b\in P$ of order s modulo p the following is true: $s\mid r$, because from **Theorem 3(2).** $\exists c\in P$ of order $lcm[r;s]$ modulo p. If $s\nmid r$, then $lcm[r;s]>r \implies$ Contradiction with the definition of r as being of the greatest order.
$\implies$ The order of every number in P modulo p divides r. Thus, $x^r\equiv 1 \pmod p$ is held for every number in P.
As p is prime, then $x^r\equiv 1 \pmod p$ has at most r different solutions in $P \implies r\ge|P|=p-1$
$\implies r=p-1=\phi(p)$ ■

Theorem 5. The number of primitive roots modulo p is $\phi(p-1)$ for p-prime.
Proof. Let x be a primitive root modulo p. Then:

$$x^{p-1}\equiv 1 \pmod p$$

The numbers $x,x^2,x^3,\ldots,x^{p-1}$ form a complete system of remainders modulo p, because if we suppose the opposite: $x^s\equiv x^r \pmod p$, then $p\mid x^s-x^r=x^r(x^{s-r}-1)$ (W.L.G. $s>r$) $\implies x^{s-r}\equiv 1 \pmod p$, which is a contradiction with **Definition 1.**
From **Theorem 2.** the number x^k is of order $\dfrac{p-1}{gcd(k;p-1)}$, which is equal to $p-1 \iff gcd(k;p-1)=1$. Hence, the number of these numbers k is $\phi(p-1)$ ■

Item 1c. *Solution.* From **Theorem 4.** $\implies f(p)=\phi(p)=p-1$ for p-prime.
From **Theorem 5.** $\implies g(p)=\phi(\phi(p))=\phi(p-1)$ for p-prime
From **Item 1a.** $\implies f(n)\le g(n)$
If n is composite, then there exists a divisor d of n so that: $d<n$
$\implies \phi(n)\le n-2$
$f(n)=n-1\le\phi(n)\le n-2 \implies$ Contradiction.
$\implies f(n)<n-1$ for every composite number n. ■

Theorem 6. There exists a primitive root modulo p^m for every odd p and $m\in\mathbb{Z}^+$
Proof. The theorem is proved for $m=1$. Let $m>1$.

Step 1. We are going to prove that there exists a number a of order $p-1$ modulo p^m.
Let a_0 be a primitive root modulo $p \implies a_0^{p-1} \equiv 1 \pmod{p}$ and $a_0^r \not\equiv 1 \pmod{p}$ for every $1 \leq r < p-1$
$a_0^p \equiv a \pmod{p}$, $a_0^{p^2} \equiv a_0^p \equiv a_0 \pmod{p} \ldots a_0^{p^{m-1}} \equiv a_0 \pmod{p}$
Let $a = a_0^{p^{m-1}}$, $a \equiv a_0 \pmod{p}$
From **Euler's Theorem** $\implies a_0^{\phi(p^m)} \equiv 0 \pmod{p^m}$, i.e. $a_0^{p^{m-1}(p-1)} \equiv 1 \pmod{p^m}$
$\implies a^{p-1} \equiv 1 \pmod{p^m}$
Let's suppose that there exists $r \in \mathbb{Z}^+$ and $r < p-1$, for which $a^r \equiv 1 \pmod{p}$
$\implies a^r \equiv 1 \pmod{p}$, but $a \equiv a_0 \pmod{p} \implies a_0^r \equiv 1 \pmod{p} \implies$ Contradiction.
Thus, $p-1$ is the order of a modulo p^m.
Step 2. We are going to prove that there exists a number b of order p^{m-1} modulo p^m
We are going to use induction to prove that $(1+p)^{p^j} \equiv 1 + p^{j+1} \pmod{p^{j+2}}$ for $j \in \mathbb{Z}_0^+$

Base. $j = 0$ $(1+p)^1 \equiv 1 + p^1 \pmod{p^2}$

Induction hypothesis. Suppose it is true for some j:

$$(1+p)^{p^j} = 1 + p^{j+1} + sp^{j+2}, s \in \mathbb{Z}$$

Inductive step. For $j+1$:

$$(1+p)^{p^{j+1}} = \left(1 + (1+sp)p^{j+1}\right)^p$$

$$\left(1 + (1+sp)p^{j+1}\right)^p = \sum_{i=0}^{p} \left[\binom{p}{i} 1^{p-i} \left((1+sp)p^{j+1}\right)^i\right]$$

$\binom{p}{i} = \dfrac{p!}{(p-i)!i!}$ is divisible by p for every $i \in \{1, 2, \ldots, p-1\}$, because $p \nmid (p-i)!$ and $p \nmid i!$

$$\implies \left(1 + (1+sp)p^{j+1}\right)^p \equiv 1 + p^{j+2} \pmod{p^{j+3}}$$

The statement is proven by induction.
For $j = m-1$ we get that:

$$(1+p)^{p^{m-1}} \equiv 1 + p^m \pmod{p^{m+1}}$$
$$\implies (1+p)^{p^{m-1}} \equiv 1 \pmod{p^m}$$

For $j = m-2$ we get that:

$$(1+p)^{p^{m-2}} \equiv 1 + p^{m-1} \pmod{p^m}$$

And $1 + p^{m-1} \not\equiv 1 \pmod{p^m}$

$\implies$ The order of $b = p+1$ is a divisor of p^{m-1} (From **Theorem 1.**) and is greater than $p^{m-2} \implies$ The order is exactly p^{m-1}.
From **Step 1.** and **Step 2.**, using **Theorem 3(1).**, and because $gcd(p-1; p^{m-1}) = 1 \implies$ The number ab is of order:

$$p^{m-1}(p-1) = \phi(p^m)$$

■

Corollary 1. *of Theorem 6.* For every odd prime p and every $m \in \mathbb{Z}^+$ there exists a primitive root for $n = 2p^m$.
Proof. If g is a primitive root modulo p^m, then $g + p^m$ is too. Let h be the odd number of these two. Because $\phi(n)$ is multiplicative, $\phi(2p^m) = \phi(2)\phi(p^m) = \phi(p^m)$
$h^{\phi(p^m)} \equiv 1 \pmod{p^m} \implies p^m \mid h^{\phi(p^m)} - 1$ and h is odd $\implies 2p^m \mid h^{\phi(2p^m)} - 1 \implies h$ is a primitive root modulo $2p^m$ ■

Item 1d. *Solution.* From **Theorem 6.** $\implies f(p^m) = \phi(p^m) = p^{m-1}(p-1)$ for every odd prime p.
Algorithm 1. Let x be a known element of maximal order modulo n.
The numbers $x, x_1, x_2, x_3, \ldots, x^{f(n)}$ have pairwise different remainders modulo n (proven in **Theorem 5.**)
The order modulo n of the number $x^k, k \in \{1, 2, \ldots, f(n)-1\}$ is $\dfrac{f(n)}{gcd(k, f(n))}$ (from **Theorem 2.**), which is equal to $f(n) \iff gcd(k; f(n)) = 1$
Calculating these powers gives us $\phi(f(n))$ elements of maximal order modulo n, including x. This algorithm generates all the elements of maximal order for primes (from **Theorem 5.**). ■

Item 1e. **Theorem 7.** The number 2^α has a primitive root only for $\alpha = 1$ or $\alpha = 2$

Proof
$\alpha = 1 \implies \phi(2) = 1 = f(2)$ (from **Item 1b.**)
$\alpha = 2 \implies \phi(4) = 2 = f(4)$ (from **Item 1b.**)
Let α be greater than 2. We are going to prove by induction that $a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$ for every odd α

Base. $\alpha = 3$ $a^2 - 1 = (a-1)(a+1)$

$(a-1)$ and $(a+1)$ are two consecutive even numbers.

Therefore, one is divisible by four. $\implies 8 \mid a^2 - 1$

Induction hypothesis. Suppose it is true for α :

$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$

Inductive step. For $\alpha + 1$: $\quad a^{2^{\alpha-1}} - 1 = (a^{2^{\alpha-2}} - 1)(a^{2^{\alpha-2}} + 1)$

From the hypothesis $2^\alpha \mid a^{2^{\alpha-2}} - 1$

$(a^{2^{\alpha-2}} + 1)$ is even $\implies 2^{\alpha+1} \mid a^{2^{\alpha-1}} - 1$

The theorem is proved. ■

Corollary 2. *of Theorem 7.* $f(2^\alpha) = 2^{\alpha-2}$

Proof. We are going to prove by induction that $2^\alpha \nmid 3^{2^{\alpha-3}} - 1$ for $\alpha \geq 4$

Base. $\alpha = 4$ $16 \nmid 9 - 1$

Induction hypothesis. Suppose it is true for α :

$2^\alpha \nmid 3^{2^{\alpha-3}} - 1$

Inductive step. For $\alpha + 1$:

$3^{2^{\alpha-2}} - 1 = (3^{2^{\alpha-3}} - 1)(3^{2^{\alpha-3}} + 1)3^{2^{\alpha-3}} \equiv (-1)^{2^{\alpha-3}} \equiv 1 \pmod 4$

$\implies 2 \mid 3^{2^{\alpha-3}} + 1$ and $4 \nmid 3^{2^{\alpha-3}} + 1$

From **Theorem 7.** $\implies 2^{\alpha-1} \mid 3^{2^{\alpha-3}} - 1$

From the hypothesis $\implies 2^\alpha \nmid 3^{2^{\alpha-3}} - 1$

$\implies 2^\alpha \mid 3^{2^{\alpha-2}} - 1$ and $2^{\alpha-1} \nmid 3^{2^{\alpha-2}} - 1$

The induction is done.
$\implies 3^{2^{\alpha-3}} \not\equiv 1 \pmod{2^\alpha}$
Let's check for $\alpha = 3$: $3^1 \not\equiv 1 \pmod 8$
From **Theorem 1.** $\implies$ The order of 3 divides $2^{\alpha-2}$ and is greater than $2^{\alpha-3}$ $\implies$ It is exactly $2^{\alpha-2}$ $\implies$ $f(2^\alpha) = 2^{\alpha-2}$ for every $\alpha \geq 3$ ■

We have proved so far that:
$f(p^m) = f(2p^m) = \phi(p^m)$ for every odd prime p and $m \in \mathbb{Z}^+$
$f(2) = 1$, $f(4) = 2$ and $f(2^\alpha) = 2^{\alpha-2}$ (for $\alpha \geq 3$)
Theorem 8. For every other n: $n \neq 2$, $n \neq 4$, $n \neq p^m$ and $n \neq 2p^m$, there are no primitive roots.
Proof. Let n not be of the aforementioned forms and $n \neq 2^\alpha$, for which the statement is already proved.
$\implies$ n can be written as $n = n_1 n_2$, $gcd(n_1; n_2) = 1$ and $n_1 > 2$, $n_2 > 2$.
Let a be a random integer coprime to n.
$\phi(n_1)$ and $\phi(n_2)$ are even (follows directly from the formula for $\phi(n)$) $\implies$

They are not coprime $\implies k = lcm[\phi(n_1); \phi(n_2)] < \phi(n_1)\phi(n_2) = \phi(n_1 n_2) = \phi(n)$
As $gcd(a; n) = 1 \implies a^{\phi(n_1)} \equiv 1 \pmod{n_1}$ and $a^{\phi(n_2)} \equiv 1 \pmod{n_2}$
$\implies a^k \equiv 1 \pmod{n}$, but $k < \phi(n)$. Thus, according to **Definition 1.** the theorem is proved. ■

From **Theorem 8.** $\implies f(n) < \phi(n)$ for the described n
From **Theorem 1.** $\implies f(n) \mid \phi(n)$ and $\phi(n)$ is even
$\implies f(n) = \frac{\phi(n)}{m}$, where m is a divisor of $\phi(n)$ and $m \geq 2$

Theorem 9. $g(n) = \phi(\phi(n))$, when n has a primitive root.
Proof. From **Algorithm 1.** $\implies g(n) \geq \phi(\phi(n))$
Let x be a primitive root
$x, x^2, \ldots, x^{\phi(n)}$ are $\phi(n)$ different remainders. The remainders, which have order defined for them, are all coprime to $n \implies$ Their count is exactly $\phi(n) \implies g(n) \leq \phi(\phi(n)) \implies g(n) = \phi(\phi(n))$ ■

Item 2b. Here are the values of $f(n)$, $g(n)$ and the numbers of maximal order for $n \leq 10$ and $n \in \mathbb{Z}[i]$.

f(2)=2, g(2)=1, [i]
f(3)=8, g(3)=4, [1+i, 1+2i, 2+i, 2+2i]
f(4)=4, g(4)=4, [i, 3i, 2+i, 2+3i]
f(5)=4, g(5)=12, [i, 4i, 1+i, 1+4i, 2, 2+2i, 2+3i, 3, 3+2i, 3+3i, 4+i, 4+4i]
f(6)=8, g(6)=8, [1+2i, 1+4i, 2+i, 2+5i, 4+i, 4+5i, 5+2i, 5+4i]
f(7)=48, g(7)=16, [1+2i, 1+3i, 1+4i, 1+5i, 2+i, 2+6i, 3+i, 3+6i, 4+i, 4+6i, 5+i, 5+6i, 6+2i, 6+3i, 6+4i, 6+5i]
f(8)=4, g(8)=24, [i, 3i, 5i, 7i, 1+2i, 1+6i, 2+i, 2+3i, 2+5i, 2+7i, 3+2i, 3+6i, 4+i, 4+3i,4+5i, 4+7i, 5+2i, 5+6i, 6+i, 6+3i, 6+5i, 6+7i, 7+2i, 7+6i]
f(9)=24, g(9)=32, [1+i, 1+2i, 1+4i, 1+5i, 1+7i, 1+8i, 2+i, 2+4i, 2+5i, 2+8i, 4+i, 4+2i, 4+4i, 4+5i, 4+7i, 4+8i, 5+i, 5+2i, 5+4i, 5+5i, 5+7i, 5+8i, 7+i, 7+4i, 7+5i, 7+8i, 8+i, 8+2i, 8+4i, 8+5i, 8+7i, 8+8i]
f(10)=4, g(10)=24, [i, 9i, 1+4i, 1+6i, 2+3i, 2+5i, 2+7i, 3, 3+2i, 3+8i, 4+i, 4+9i, 5+4i, 5+6i, 6+i, 6+9i, 7, 7+2i, 7+8i, 8+3i, 8+5i, 8+7i, 9+4i, 9+6i