TECHNICAL TRANSACTIONS 11/2017
CZASOPISMO TECHNICZNE 11/2017

MATHEMATICS

DOI: 10.4467/2353737XCT.17.194.7423

Maciej Zakarczemny (mzakarczemny@pk.edu.pl)
Institut of Matchematics, Faculty of Physis, Mathematics and Computer Science, Cracow University of Technology

Lower and upper bounds for solutions of the congruence $x^m \equiv a (\mathrm{mod}\ n)$

Dolne oszacowanie na największe i górne oszacowanie na najmniejsze rozwiązanie kongruencji $x^m \equiv a (\mathrm{mod}\ n)$

Abstract

Let n, m be natural numbers with $n \geq 2$. We say that an integer a, $(a, n) = 1$, is the m-th power residue modulo n if there exists an integer x such that $x^m \equiv a (\mathrm{mod}\ n)$. Let $C(n)$ denote the multiplicative group consisting of the residues modulo n which are relatively prime to n. Let $s(n, m, a)$ be the smallest solution of the congruence $x^m \equiv a (\mathrm{mod}\ n)$ in the set $C(n)$. Let $t(n, m, a)$ be the largest solution of the congruence $x^m \equiv a (\mathrm{mod}\ n)$ in the set $C(n)$. We will give an upper bound for $s(n, m, a)$ and a lower bound for $t(n, m, a)$.

Keywords: smallest solution, largest solution, upper bound, lower bound, congruence relation, residue class, n-th degree equation

Streszczenie

Niech n, m będą liczbami naturalnymi, takimi że $n \geq 2$. Powiemy, że liczba całkowita a, $(a, n) = 1$, jest m-tą resztą kwadratową modulo n, jeśli istnieje liczba całkowita x, taka że $x^m \equiv a (\mathrm{mod}\ n)$. Niech $C(n)$ będzie grupą multiplikatywną zawierającą reszty modulo n, względnie pierwsze z n. Oznaczmy przez $s(n, m, a)$ najmniejsze rozwiązanie równania $x^m \equiv a (\mathrm{mod}\ n)$ w zbiorze $C(n)$. Oznaczmy przez $t(n, m, a)$ największe rozwiązanie równania $x^m \equiv a (\mathrm{mod}\ n)$ w zbiorze $C(n)$. Podamy górne oszacowanie na $s(n, m, a)$ oraz dolne na $t(n, m, a)$.

Słowa kluczowe: najmniejsze rozwiązanie, największe rozwiązanie, górne oszacowanie, dolne oszacowanie, kongruencja, klasa reszt, równanie wielomianowe

1. Introduction

Let n, m be natural numbers with $n \geq 2$. Let a be an integer, with $(a, n) = 1$. By $s(a, n, m)$, $t(a, n, m)$ we denote, correspondingly, the smallest and largest solutions of the congruence $x^m \equiv a \pmod{n}$, where $1 \leq x \leq n - 1$. We will give an upper bound for $s(n, m, a)$ and a lower bound for $t(n, m, a)$. Let $C(n)$ denote the multiplicative group consisting of residues modulo n, which are relatively prime to n (reduced set of residues modulo n).

Let $C_k(n)$ denote the subgroup of $C(n)$ consisting of k-th powers.

Denote $v_k(n) = [C(n): C_k(n)]$. Let n have prime factorization $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}$, where $a_j \geq 1$. By [2]:

$$v_k(n) = v_k\left(p_1^{a_1}\right) \cdot v_k\left(p_2^{a_2}\right) \cdot \ldots \cdot v_k\left(p_r^{a_r}\right),$$

$$v_k(2) = 1,\ v_k(2^\alpha) = (k, 2)(k, 2^{\alpha-2}),\ \text{for } \alpha \geq 2.$$

If p is an odd prime and $\alpha \geq 1$, then $v_k(p^\alpha) = (k, \varphi(p^\alpha))$. Also $v_k(n) \leq 2k^r$.

Definition 1.1. Let

$$1 = g_0(n,k) < g_1(n,k) < \ldots < g_{v-1}(n,k), \tag{1}$$

be the smallest positive representatives of the $v = v_k(n)$ cossets of $C_k(n)$.

Definition 1.2. Let

$$w_0(n,k) < w_1(n,k) < \ldots < w_{v-1}(n,k) = n - 1, \tag{2}$$

be the largest positive representatives of the $v = v_k(n)$ cossets of $C_k(n)$.

By Norton [2] we have:

Theorem 1.3. If n, k are positive integers $0 \leq i \leq v - 1$, then

$$g_i(n,k) \leq 1 + \frac{n}{\varphi(n)}\left(2^{\omega(n)}\right)^{\frac{3}{2}}\left(\frac{iv}{v-i}\right)^{\frac{1}{2}} n^{\frac{1}{2}} \log n, \tag{3}$$

where $\omega(n)$ is the number of distinct prime divisors of n.

See [2].

Corollary 1.4. For each $\varepsilon > 0$

$$g_{v-1}(n,k) = O\left(n^{\frac{1}{2}+\varepsilon}\right), \tag{4}$$

where the implied constant depends only on k, ε and the number of distinct prime factors of n. See [2].

Corollary 1.5. If p, q, r are odd distinct prime numbers and α, β, γ are positive integers, then

$$g_{\nu-1}(n,k)<\begin{cases}1+3\sqrt{2}k\sqrt{n}\log n & \text{if} \quad n=p^{\alpha}, \\ 1+24k\sqrt{n}\log n & \text{if} \quad n=2p^{\alpha}, \\ 1+8\sqrt{2}k\sqrt{n}\log n & \text{if} \quad n=2^{\alpha}, \alpha\geq 2, \\ 1+15k^{2}\sqrt{n}\log n & \text{if} \quad n=p^{\alpha}q^{\beta}, \\ 1+35\sqrt{2}k^{3}\sqrt{n}\log n & \text{if} \quad n=p^{\alpha}q^{\beta}r^{\gamma}.\end{cases} \tag{5}$$

Proof. By theorem 1.3.

2. Theorems

The following theorem shows the relationship between $g_i(n, k)$ and $w_{\nu-1-i}(n, k)$.

Theorem 2.1. For $0 \leq i \leq \nu - 1$, we have

$$g_i(n,k)+w_{\nu-1-i}(n,k)=n. \tag{6}$$

Proof. Let us note that

$$n-g_i(n,k)\in g_j(n,k)C_k(n) \quad \text{iff} \quad g_i(n,k)\in(n-g_j(n,k))C_k(n), \tag{7}$$

where $0 \leq i, j \leq \nu - 1$.

We define a permutation $\sigma:\{0,1,\ldots,\nu-1\}\to\{0,1,\ldots,\nu-1\}$ by the relation

$$(n-g_i(n,k))C_k(n)=g_j(n,k)C_k(n)=w_{\sigma(i)}(n,k)C_k(n). \tag{8}$$

Then by definition of $w_{\sigma(i)}(n, k)$ we have

$$n-g_i(n,k)\leq w_{\sigma(i)}(n,k). \tag{9}$$

On the other hand

$$(n-w_{\sigma(i)}(n,k))C_k(n)=(n-g_j(n,k))C_k(n)=g_i(n,k)C_k(n). \tag{10}$$

Hence by definition of $g_i(n, k)$ we get

$$g_i(n,k) \le n - w_{\sigma(i)}(n,k). \tag{11}$$

Therefore by (9), (11)

$$g_i(n,k) + w_{\sigma(i)}(n,k) = n. \tag{12}$$

Using (1) we obtain

$$w_{\sigma(v-1)}(n,k) < w_{\sigma(v-2)}(n,k) < \ldots < w_{\sigma(1)}(n,k) < w_{\sigma(0)}(n,k) = n-1, \tag{13}$$

hence by (2)

$$\sigma(i) = \nu - 1 - i, \tag{14}$$

and we are finished.

Using theorem 1.3 and theorem 2.1 we get the following lower bound on $w_i(n, k)$.

Theorem 2.2. If n, k are positive integers $0 \le i \le v - 1$, then

$$w_i(n,k) \ge n - 1 - \frac{n}{\varphi(n)}\left(2^{\omega(n)}\right)^{\frac{3}{2}}\left(\frac{(v-1-i)v}{i+1}\right)^{\frac{1}{2}} n^{\frac{1}{2}} \log n. \tag{15}$$

Proof. By theorem 2.1 and theorem 1.3.

It follows that

Remark 2.3.

$$n - w_0(n,k) = O\left(n^{\frac{1}{2}+\varepsilon}\right), \tag{16}$$

for each $\varepsilon > 0$, where the implied constant depends only on k, ε and the number of distinct prime factors of n.

Finally, in the proof of the following theorem, we will show how to reduce the problem of finding bounds for $s(a, n, m)$, $t(a, n, m)$ to the problem of finding bounds for $g_i(n, k)$ and $w_i(n, k)$.

Theorem 2.4. Let n, m be natural numbers such that $n \ge 2$. Let a be an integer relatively prime to n, which is m-th power residue modulo n. By $s(a, n, m)$, $t(a, n, m)$ we denote, correspondingly, the smallest and the largest solution of the congruence

$$x^m \equiv a \pmod{n}, \tag{17}$$

where $1 \le x \le n - 1$. Then

$$s(a,n,m)\le 1+\frac{n}{\varphi(n)}\left(2^{\omega(n)}\right)^{\frac{3}{2}}\left(v(v-1)\right)^{\frac{1}{2}}n^{\frac{1}{2}}\log n, \qquad (18)$$

$$t(a,n,m)\ge n-1-\frac{n}{\varphi(n)}\left(2^{\omega(n)}\right)^{\frac{3}{2}}\left(v(v-1)\right)^{\frac{1}{2}}n^{\frac{1}{2}}\log n, \qquad (19)$$

where $v=v_{\frac{\varphi(n)}{(\varphi(n),m)}}(n)$.

Proof. It is sufficient to consider equation $x^m = a$ in the group $C(n)$. Let $k=\frac{\varphi(n)}{(\varphi(n),m)}$. We may assume that there exist $0 \le i_0, j_0 \le v-1$ such that

$$s(a,n,m)\in g_{i_0}(n,k)C_k(n), \qquad (20)$$

$$t(a,n,m)\in w_{j_0}(n,k)C_k(n), \qquad (21)$$

since $s(a, n, m), t(a, n, m) \in C(n)$.

By definition of $g_{i_0}(n,k)$ and $w_{j_0}(n,k)$ we obtain

$$s(a,n,m)\ge g_{i_0}(n,k), \qquad (22)$$

$$t(a,n,m)\le w_{j_0}(n,k). \qquad (23)$$

On the other side

$$g_{i_0}(n,k)\in s(a,n,m)C_k(n), \qquad (24)$$

$$w_{j_0}(n,k)\in t(a,n,m)C_k(n), \qquad (25)$$

hence, there exist $\lambda, \theta \in C(n)$ such that

$$g_{i_0}(n,k)=s(a,n,m)\lambda^k, \qquad (26)$$

$$w_{j_0}(n,k)=t(a,n,m)\theta^k. \qquad (27)$$

But $(\varphi(n),m)|m,$ thus by Euler's theorem we obtain

$$g_{i_0}(n,k)^m=s(a,n,m)^m\lambda^{km}=a\left(\lambda^{\frac{m}{(\varphi(n),m)}}\right)^{\varphi(n)}=a, \qquad (28)$$

$$w_{j_0}(n,k)^m = t(a,n,m)^m \theta^{km} = a\left(\theta^{\frac{m}{(\varphi(n),m)}}\right)^{\varphi(n)} = a, \tag{29}$$

hence $g_{i_0}(n,k)$ and $w_{j_0}(n,k)$ are solutions of the equation $x^m = a$ in the group $C(n)$.
By definition of $s(a, n, m)$, $t(a, n, m)$, we get

$$s(a,n,m) \le g_{i_0}(n,k), \tag{30}$$

$$t(a,n,m) \ge w_{j_0}(n,k). \tag{31}$$

By (22), (23), (30), (31)

$$s(a,n,m) = g_{i_0}(n,k), \tag{32}$$

$$t(a,n,m) = w_{j_0}(n,k). \tag{33}$$

By theorem 1.3 and theorem 2.2 we get

$$s(a,n,m) = g_{i_0}(n,k) \le g_{v-1}(n,k) \le 1 + \frac{n}{\varphi(n)}\left(2^{\omega(n)}\right)^{\frac{3}{2}}\left(v(v-1)\right)^{\frac{1}{2}} n^{\frac{1}{2}} \log n, \tag{34}$$

$$t(a,n,m) = w_{j_0}(n,k) \ge w_0(n,k) \ge n - 1 - \frac{n}{\varphi(n)}\left(2^{\omega(n)}\right)^{\frac{3}{2}}\left(v(v-1)\right)^{\frac{1}{2}} n^{\frac{1}{2}} \log n. \tag{35}$$

Corollary 2.5. Under the assumptions of theorem 2.4 we have that

$$s(a,n,m) \le 1 + \frac{n}{\varphi(n)}\left(2^{\omega(n)}\right)^{\frac{3}{2}} v n^{\frac{1}{2}} \log n, \tag{36}$$

$$t(a,n,m) \ge n - 1 - \frac{n}{\varphi(n)}\left(2^{\omega(n)}\right)^{\frac{3}{2}} v n^{\frac{1}{2}} \log n. \tag{37}$$

Remark 2.6. If $m = \varphi(n)$, then $a = 1$, $k = 1$ $C_1(n) = C(n)$, $v_1 = 1$, $s(1, n, \varphi(n)) = 1$, $t(1, n, \varphi(n)) = n - 1$. In fact, we get optimal bounds using (18) and (19).

Remark 2.7. We may assume that $m \mid \varphi(n)$. Indeed, let d be a natural number such that $d \cdot \frac{m}{(\varphi(n),m)} \equiv 1(\operatorname{mod} \varphi(n))$, we have equivalent congruencies

$$x^m \equiv a(\operatorname{mod} n) \text{ if } x^{(\varphi(n),m)} \equiv a^d(\operatorname{mod} n). \tag{38}$$

Thus $s(a,n,m)=s\left(a^d,n,(\varphi(n),m)\right), t(a,n,m)=t\left(a^d,n,(\varphi(n),m)\right)$.
Note that the left-hand side of inequalities (18), (19) does not depend on a.

Remark 2.8. Let $n = p^{\alpha}$, where p is an odd prime and α is a positive integer. We may assume that $m|\varphi(n)$, (see remark 2.7). Then

$$v=v_{\frac{\varphi(n)}{(\varphi(n),m)}}(n)=v_{\frac{\varphi(n)}{m}}(n)=\left(\frac{\varphi(n)}{m},\varphi(n)\right)=\frac{\varphi(n)}{m}. \tag{39}$$

By corollary 2.5

$$s(a,n,m)\leq 1+2\sqrt{2}\frac{n^{\frac{3}{2}}\log n}{m},\ t(a,n,m)\geq n-1-2\sqrt{2}\frac{n^{\frac{3}{2}}\log n}{m}. \tag{40}$$

Remark 2.9. Let $n = 2^{\alpha}$, where α is a positive integer greater or equal 2. We may assume that $m|\varphi(n)$. and $m<\varphi(n)=2^{\alpha-1}$ (see remarks 2.7 and 2.6). Then

$$v=v_{\frac{\varphi(n)}{(\varphi(n),m)}}(n)=v_{\frac{\varphi(n)}{m}}(n)=\left(\frac{\varphi(n)}{m},2\right)\left(\frac{\varphi(n)}{m},2^{\alpha-2}\right)=2\frac{\varphi(n)}{m}. \tag{41}$$

By corollary 2.5

$$s(a,n,m)\leq 1+4\sqrt{2}\frac{n^{\frac{3}{2}}\log n}{m},\ t(a,n,m)\geq n-1-4\sqrt{2}\frac{n^{\frac{3}{2}}\log n}{m}. \tag{42}$$

We will now give an application of theorem 2.4.

Theorem 2.10. Let p be an odd prime number. For the congruence

$$x^{\frac{p-1}{2}}\equiv -1(\bmod p), 1\leq x\leq p-1, \tag{43}$$

we have that:

1) the congruence (43) has a solution, i.e. -1 is $\frac{p-1}{2}$-th power residue modulo p,

2) the smallest solution $s\left(-1,p,\frac{p-1}{2}\right)$ is a prime number,

3) $s\left(-1,p,\frac{p-1}{2}\right)\leq 1+4\frac{p}{p-1}p^{\frac{1}{2}}\log p$,

4) the largest solution $t\left(-1,p,\frac{p-1}{2}\right) \geq p-1-4\frac{p}{p-1}p^{\frac{1}{2}}\log p.$

Proof. If g is a primitive root modulo p (such primitive root exists, since p is a prime number), then $g^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ and $g^{p-1} \equiv 1 \pmod{p}$. Hence $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ and 1) holds.

If $s\left(-1,p,\frac{p-1}{2}\right)$ were a composite number, it could be expressed as $s\left(-1,p,\frac{p-1}{2}\right) = s = ab$ where $a,b \in \mathbb{N}, a,b > 1$. Note that $a^{\frac{p-1}{2}} \not\equiv -1 \pmod{p}$ and $b^{\frac{p-1}{2}} \not\equiv -1 \pmod{p}$, since s is the smallest solution of the congruence (43). By Fermat's little theorem, we know that $a^{p-1} \equiv 1 \pmod{p}$ and $b^{p-1} \equiv 1 \pmod{p}$. Hence $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ and $b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Thus $s^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, a contradiction with definition of s.

Therefore the initial assumption, that s is a composite number, must be false. Hence 2) holds.

We have $k = \dfrac{\varphi(p)}{\left(\varphi(p), \frac{p-1}{2}\right)} = 2, v = v_2(p) = (2, \varphi(p)) = 2, \left(2^{\omega(p)}\right)^{\frac{3}{2}} \left(v(v-1)\right)^{\frac{1}{2}} = 4.$

Thus 3) and 4) follows by theorem 2.4.

Example 2.11. For the congruence $x^{359} \equiv -1 \pmod{719}$, we have

$$s(-1,719,359) = 11, \quad t(-1,719,359) = 718, \tag{44}$$

in this case theorem 2.10, says that $s(-1,719,359)$ is a prime number and

$$s(-1,719,359) \leq 707, \quad t(-1,719,359) \geq 12.$$

References

[1] Nathanson M.B., *Elementary Methods in Number Theory*, Vol. 195, GTM, Springer, New York 2000.

[2] Norton K.K., *k-th coset representatives modulo n*, Acta Arithmetica, XV, 1969, 161-179.