3. Barrett P.D. Implementing the Rivest Shamir and Adleman Public Key Encryption algorithm on a Standard Digital Signal Processor // Advances in Cryptology. EUROCRYPT `86. Lect. Notes Comput. Sci. -1987. -№ 263.- P.311-323.
4. Bosselaers A., Govaerts R., Vandawalle J. Comparison of Three Modular Reduction Function // Advances in Cryptology. EUROCRYPT ` 94. Lect. Notes Comput. Sci. -1994. -№ 773. -P. 175-186.
5. Задирака В.К., Абдикаликов К.А. Элементы современной криптологии и методы защиты банковской информации. –Алматы.: Гылым, 1999. -336с.

Түйін

Мақалада көпразрядты бүтін сандармен жасалатын операцияларда қолданылатын модулярлы арифметиканы есептеудің тиімді әдістері ұсынылған.

Resume

In the paper we propose effective methods for calculating the modular arithmetic used in operations with multi-digit whole numbers.

Özet

Yazıda çok basamaklı tam sayılar ile operasyonlarda kullanılan modüler aritmetik hesaplamak için etkili yöntemler öneriyoruz.

Sh. N. Kuttykozhaeva
Doctor of physical and mathematical science
Kokshetau State University named after Sh. Ualikhanov
Kokshetau /Kazakhstan

Mathematical modelling of the tasks of hydrodynamics by the method of fictitious areas

The fictitious domain method is one of the known methods of approximate solutions of boundary value problems in mathematical physics. In general fictitious domain method is justified for the linear boundary value problems of mathematical physics. In this work is devoted to substantiation of the fictitious domain method for nonlinear elliptic equations. A new method of obtaining best possible rate of convergence of solutions in the method of fictitious domains.

Let's consider the boundary value problem for nonlinear elliptic equations in $\Omega \subset R^3$ area with border area S

$$\Delta v - v^3 = f, \qquad (1)$$

$$v|_S = 0. \qquad (2)$$

As method of fictitious domains for the continuation of the lower coefficient in the auxiliary area $D \supset \Omega$ with border $S_1, S_1 \cap S = \emptyset$, solving equation with small parameter

$$\Delta v^\varepsilon - \left(v^\varepsilon\right)^3 - \frac{\xi(x)}{\varepsilon} v^\varepsilon = f, \qquad (3)$$

$$v^\varepsilon\Big|_{S_1} = 0, \qquad (4)$$

where f - continued with zero out of Ω and $\xi(x) = \begin{cases} 0, & x \in \Omega, \\ 1, & D_1 = D \setminus \Omega. \end{cases}$

Next one notations used are from the monograph

Definition 2.1.1. Generalized solution of the exercises (3), (4) is the function $v^{\varepsilon} \in \overset{0}{W}{}_2^1(D)$, that is satisfying the integral identity

$$\left(v_x^{\varepsilon}, \Phi_x\right)_{L_2(D)} + \left(\left(v^{\varepsilon}\right)^3, \Phi\right)_{L_2(D)} + \frac{1}{\varepsilon}\left(v^{\varepsilon}, \Phi\right)_{L_2(D_1)} = -\left(f, \Phi\right)_{L_2(D)} \qquad (5)$$

for all $\Phi \in \overset{0}{W}{}_2^1(D)$.

Theorem 1. Let's $f \in W_2^{-1}(D)$. Then there exists a unique weak solution (3)-(4) and it is satisfied the estimate

$$\left\|v_x^{e}\right\|_{L_2(D_1)}^2 + \left\|v^{\varepsilon}\right\|_{L_4(D)}^4 + \frac{1}{\varepsilon}\left\|v^{\varepsilon}\right\|_{L_2(D_1)}^2 \leq C\|f\|_{W_2^{-1}(D)}^2, \qquad (6)$$

where $\left\|f^{\varepsilon}\right\|_{W_2^{-1}(D)} = \sup\limits_{\|\psi\|_{\overset{0}{W}{}_2^1(D)}=1} (f, \psi)_{L_2(D)}$,

at that, when $\varepsilon \to 0$ this solution converges to the generalized solution of the problem (1), (2).

Definition 2. Stronger solution of the problem (3)-(4) is called function $v^{\varepsilon} \in \overset{0}{W}{}_2^1(D) \cap W_2^2(D)$, that satisfying to equation (3) almost everywhere.

Theorem 2.1.2. Let's $f \in L_2(\Omega)$, $S, S_1 \in C^2$. Then there a stronger solution of the problem (3)-(4) and it is satisfied the estimate

$\left\|v^{\varepsilon}\right\|_{W_2^2(D) \cap \overset{0}{W}{}_2^1(D)} \leq C_{\varepsilon}$, where $C_{\varepsilon} \to \infty$, at $\varepsilon \to 0$. (7)

Theorem 2. Let's $f \in L_2(D)$, S, $S \in C^2$. Then

$$\left\|v^{\varepsilon} - v\right\|_{L_2(\Omega)} \leq C_0\sqrt{\varepsilon} \qquad (8)$$

C_0 - positive constant that not depend from ε.

References:

1. Kuttykozhayeva Sh.N. On an approximate method of solving the equation of Navier-Stokes. Vestnik KazSU, Mech.-mat Ifn., 1998.№2(14). p. 163-172.

2. Kuttykozhayeva Sh.N. The method of fictitious domains for Navier-Stokes equations. Вестник КазГУ, Vestnik KazSU, Mech.-mat Ifn., 1998.№13. p. 54-59.

3. Kuttykozhayeva Sh.N. A variant of the method of fictitious domains for the models of inhomogeneous fluids. Vestnik KazSU, Mech.-mat Ifn., 1999.№(15).

4. Samarskii A.A. Theory of different Scheme. Science. 1997. p.653.

5. Samarskii A.A. Nikolayev E.S. The method of solving of the difference equations. Science. Moscow. 1978. 188 p.

Түйін

Мақалада жалған аймақ әдісінің негіздемесі беріледі. Кіші параметр нөлге ұмтылған жағдайда бастапқы проблемны қосымша проблема арқылы бейнелеудің жинақталуының жақсармайтын бағасы келтірілген.

Резюме

В этой работе дано обоснование метода фиктивных областей. Впервые получены не знаком улучшения скорости сходимости решения от вспомогательной задачи к решению исходной задачи в то время, когда малый параметр стремится к нулю.

Özet

Bu makalede hayali etki yöntem uygulanabilirliğini, önce küçük parametresi sıfır eğilimi zaman içinde asıl probleminin çözümüne yardımcı sorunun çözümleri yakınsama oranını artırması elde ediliyor.