Involutive basis for rings with zero divisors

Ph.B. Burtyka, A.V. Trepacheva
(Southern Federal University, Rostov-on-Don – Taganrog)
E-mail address: bbfilipp@ya.ru, alina1989malina@ya.ru

We introduce a notion of involutive division for rings with zero divisors. We present a generalisation of involutive algorithm by Gerdt and Blinkov for construction involutive basis for rings with zero divisors. A careful attention is given to rings of residues modulo composite number. A case study includes both known and unknown factorization of composite number.

Инволютивный базис для колец с делителями нуля

Ф.Б. Буртыка, А.В. Трепачева
(Южный федеральный университет, Ростов-на-Дону – Таганрог)
E-mail address: bbfilipp@ya.ru, alina1989malina@ya.ru

Вводится понятие инволютивного деления для колец с делителями нуля. Предлагается обобщение инволютивного алгоритма Гердта-Блинкова для построения инволютивных базисов колец с делителями нуля. Особое внимание уделено числовым кольцам вычетов по составному модулю. Рассмотрен случай известной и неизвестной факторизации составного числа.