МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра «Информационная безопасность»

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«___» _____2016 г.

РАСШИРЕННЫЙ АЛГОРИТМ ЕВКЛИДА

Методические указания по выполнению практической работы
для студентов специальностей 10.05.03, 10.05.02, 10.03.01

Курск 2016

УДК 511.17

Составитель М.А. Ефремов

Рецензент
Кандидат технических наук, доцент *М.О. Таныгин*

Расширенный алгоритм Евклида: методические указания по выполнению практической работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2016. 10 с., Библиогр.: с. 10.

Содержат основные сведения о расширенном алгоритме Евклида и его применении для нахождения линейного разложения НОД. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ).

Предназначены для студентов специальностей 10.05.03, 10.05.02, 10.03.01 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. . Уч.-изд.л. . Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Цель лабораторной работы – научиться использовать расширенный алгоритм Евклида для нахождения линейного разложения НОД.

2. ЗАДАНИЕ

Ознакомиться с теоретическим материалом. Ознакомиться с примерами решения. Выбрать свой вариант задания, построить таблицу и вычислить линейное разложение НОД.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание.
2. Изучить теоретическую часть.
3. Получить два числа.
4. Осуществить деление в столбик.
5. Построить таблицу по алгоритму Евклида.
6. Найти линейное разложение НОД для двух чисел.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Таблица.
4. Вычисление НОД.
5. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Алгоритм Евклида — эффективный алгоритм для нахождения наибольшего общего делителя двух целых чисел. В самом простом случае алгоритм Евклида применяется к паре положительных целых чисел и формирует новую пару, которая состоит из меньшего числа и разницы между большим и меньшим числом. Процесс повторяется, пока числа не станут равными. Таким образом, НОД двух чисел равен последнему отличному от нуля остатку в алгоритме Евклида.

Первое описание алгоритма находится в «Началах» Евклида, что делает его одним из старейших численных алгоритмов, используемых в наше время. Оригинальный алгоритм был предложен только для натуральных чисел и геометрических длин (вещественных чисел). Однако в XIX веке он был обобщён на другие типы чисел, такие как целые числа Гаусса и полиномы от одной переменной. Это привело к появлению в современной общей алгебре такого понятия, как евклидово кольцо. Позже алгоритм Евклида также был обобщён на другие математические структуры, такие как узлы и многомерные полиномы.

Расширенный алгоритм Евклида.

Рассмотрим теперь расширенный алгоритм Евклида. Пусть $a,b \in Z$, $d = (a,b)$. Расширенный алгоритм Евклида подсчитывает не только d, но и два числа $U, \vartheta \in Z$, таких, что

$$aU + b\vartheta = d. \qquad (*)$$

Равенство (*) называется *линейным разложением НОД*. Каждый остаток, вычисленный в процессе работы алгоритма, можно представить в виде $r_i = ax_i + by_i$, $i = \overline{1,n}$. Рассмотрим следующую последовательность такого представления остатков:

$a = bq_1 + r_1, \quad r_1 = ax_1 + by_1;$

$b = r_1q_2 + r_2, \quad r_2 = ax_2 + by_2;$

$r_1 = r_2q_1 + r_3, \quad r_3 = ax_3 + by_3;$

$r_2 = r_3q_4 + r_4, \quad r_4 = ax_4 + by_4;$

.....

$r_{n-2} = r_{n-1}q_n + r_n, \quad r_n = ax_n + by_n = d;$

$r_{n-1} = r_nq_{n+1}, \quad r_{n+1} = 0.$

Таким образом, алгоритм Евклида - это последовательное деление с остатком

$$r_{i-2} = r_{i-1}q_1 + r_i, \quad 0 \le r_i \lhd r_{i-1}, i = \overline{i,n}.$$

$$\Downarrow$$

$$r_i = r_{i-2} - r_{i-1}q_i.$$

$$r_{i-2} = ax_{i-2} + by_{i-2};$$

$$r_{i-1} = ax_{i-1} + by_{i-1}.$$

Тогда

$$r_i = ax_{i-2} + by_{i-2} - (ax_{i-1} + by_{i-1})q_i = a(x_{i-2} - x_{i-1}q_i) + b(y_{i-2} - y_{i-1}q_i) = ax_i + by_i.$$

Поэтому $x_i = x_{i-2} - x_{i-1}q_i; \quad y_i = y_{i-2} - y_{i-1}q_i, \quad i = \overline{1,n}.$

Для определения $x_i, \quad y_i, \quad i = \overline{1,n}$, необходимо знать $x_{-1}, \quad y_{-1}, \quad x_0, \quad y_0$. Они находятся из соотношений:

$$a = r_n = ax_{-1} + by_{-1}; \quad b = ax_0 + by_0.$$

Поэтому можно положить

$$x_{-1} = 1; \quad y_{-1} = 0; \quad x_0 = 0; \quad y_0 = 1. \quad d = r_n = ax_n + by_n \quad \Rightarrow \quad U = x_n, \vartheta = y_n.$$

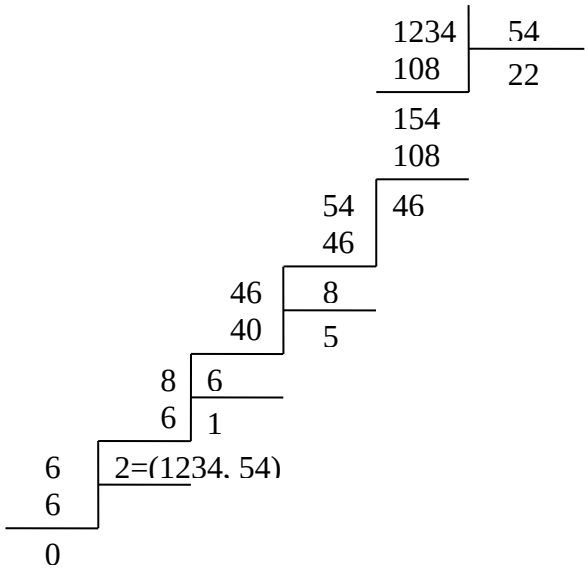
Следует отметить, что пара чисел U, ϑ не единственная. Тогда $d = aU + b\vartheta = \underline{aU} + \underline{\underline{b\vartheta}} + \underline{kab} - \underline{\underline{kab}} = a(U + kb) + b(\vartheta - ka).$

Вычисления с помощью расширенного алгоритма Евклида удобно проводить в виде таблицы.

i	Остатки	Частные	x_i	y_i
-1	a	-	1	0
0	b	-	0	1
1	r_1	q_1	$1-0*q_1=1$	$0-1*q_1=-q_1$
2	r_2	q_2	$0-1*q_2=-q_2$	$1-(-q_1)q_2=1+q_1q_2$
3	r_3	q_3	$1-(-q_2)q_3=1+q_2q_3$	$-q_1-(1+q_1q_2)q_3$
……	……	……	……	……
$n-1$	r_{n-1}	q_{n-1}	$x_{n-3}-x_{n-2}q_{n-1}$	$y_{n-3}-y_{n-2}q_{n-1}$
n	$r_n = d$	q_n	$x_{n-2}-x_{n-1}q_n = U$	$y_{n-2}-y_{n-1}q_n = \vartheta$
$n+1$	0	q_{n+1}	-	-

6. ПРИМЕР ВЫПОЛНЕНИЯ РАБОТЫ

Пример 1. Найти НОД двух чисел 1234, 54 и его разложение.



i	Остатки	Частные	x_i	y_i
-1	1234	-	1	1
0	54	-	0	0
1	46	22	1-22*0=1	0-1*22=-22
2	8	1	0-1*1=-1	1-(-22)*1=23
3	6	5	1-(-1)*5=6	-22-23*5=-137
4	2	1	-1-6*1=-7	23-(-137)*1= 160
5	0	3	-	-

$U = -7, \quad \vartheta = 160.$

Линейное разложение НОД: (1234, 54)=1234*(-7)+54*60=2.

7. ВАРИАНТЫ ЗАДАНИЙ

№ вар.	*Первое число*	*Второе число*
1	57824	2151
2	48906	3563
3	45214	2768
4	36806	7521
5	52731	6327
6	29925	4950
7	23850	1635
8	47850	4335
9	47889	1683
10	31416	3927
11	43316	2872
12	36201	7419
13	37389	2760
14	26928	5412
15	31206	1586
16	37506	2478
17	27138	6874
18	40755	3963
19	36516	3651
20	33994	3632
21	24729	4782
22	49854	5421
23	50538	2864
24	42075	3969
25	41314	3218
26	46563	4521
27	51396	2486
28	37422	3423
29	42262	3756
30	46948	3768

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Дайте определение наибольшего общего делителя.
2. Сформулируйте алгоритм Евклида для нахождения наибольшего общего делителя двух чисел.
3. Дать определение понятия "взаимно простые числа". Привести примеры взаимно простых чисел и чисел, не являющихся взаимно простыми.
4. Чему будет равен НОД взаимно простых чисел? А простых чисел?
5. Для чего используется расширенный алгоритм Евклида?
6. Что такое линейное разложение НОД?

8. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Виноградов И.М. Основы теории чисел. М.: Наука,1995.
2. Галочкин А.И., Нестеренко Н.В., Шидловский А.Б. Введение в теорию чисел. Изд - во МГУ, 1995.
3. Кудреватов Г.А. Сборник задач по теории чисел. М.: Просвещение,1970.
4. Ляпин С.Е., Баранова И.В., Борчугова З.Г. Сборник задач по элементарной математике. М.: Просвещение, 1973.
5. И.М. Виноградов «Элементы высшей математики» М., «Высшая школа», 1999
6. Л.Я. Куликов, А.И. Москаленко, А.А. Фомин «Сборник задач по алгебре и теории чисел» М., «Просвещение», 1993
7. Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Ажевич «Математические и компьютерные основы криптологии» Минск, «Новое знание», 2003