1. Простой и расширенный алгоритм Евклида

НОД (наибольший общий делитель) двух целых чисел s и r есть наибольшее целое gcd : $\quad gcd|s \bigwedge gcd|s$. Известный "школьный"метод нахождения НОД состоит в разложении обоих чисел на простые сомножители и отборе общих сомножителей. Есть гораздо более эффекивный метод - алгоритм Евклида нахождения НОД.

- 1. Даны два ненулевых целых a и b.
- 2. Выполним деление с остатком $a = q \cdot b + r$, q и r целые $0 \leq r < |b|$.
- 3. Если $r = 0$, принимаем за НОД $|b|$ и stop.
- 4. Иначе, заменим (a, b) на (b, r).
- 5. Go to Step 2.

Запишем подробнее работу этого алгоритма в нетривиальном случае $(b \nmid a)$.

$$\begin{gathered}
a = q_1 \cdot b + r_1 \quad 0 < r_1 < |b|; \\
b = q_2 \cdot r_1 + r_2 \quad 0 < r_2 < r_1; \\
r_1 = q_3 \cdot r_2 + r_3 \quad 0 < r_3 < r_2; \\
\vdots \\
r_{n-2} = q_n \cdot r_{n-1} + r_n \quad 0 < r_n < r_{n-1}; \\
r_{n-1} = q_{n+1} \cdot r_n \qquad .
\end{gathered}$$

Этот процесс закончится на каком-то шаге, т.к. каждый следующий остаток положителен, но меньше предыдущего. Имеем: $b > r_1 > r_2 > \cdots > r_n > 0$, следовательно процесс оборвется максимум через b шагов. Если $r_n = 1$, то числа взаимно просты.

Пример. Найдем НОД(525, 231). Кстати, буквы НОД в данном контексте часто опускают и пишут просто (525, 231). Все выкладки можно выполнить вот так:

$$
\begin{array}{rr|l}
 & 525 & 231 \\
\cline{3-3}
- & 462 & 2 \\
\cline{2-3}
 & 231 & 63 \\
\cline{2-3}
- & 189 & 3 \\
\cline{2-3}
 & 63 & 42 \\
\cline{2-3}
- & 42 & 1 \\
\cline{2-3}
 & 42 & 21 \\
\cline{2-3}
- & 42 & 2 \\
\cline{2-3}
 & 0 &
\end{array}
$$

Иначе:

$$
\begin{aligned}
525 &= 231 \cdot 2 + \underline{63} \\
231 &= 63 \cdot 3 + 42 \\
63 &= 42 \cdot 1 + 21 \\
42 &= 21 \cdot 2
\end{aligned}
$$

Итак, (525, 231)=21.

Очень полезным оказывается *расширенный* вариант алгоритма Евклида. Заметим, что каждый остаток r_i есть линейная комбинация предыдущих двух остатков.

$$r_1 = s - q_1 \cdot r, \quad r_2 = r - q_2 \cdot r_1, \quad \ldots, \quad r_n = r_{n-1} - q_n \cdot r_{n-1}.$$

Можно проделать обратную подстановку явно, тогда получается следующее

$$r_n = r_{n-2} - r_{n-1}q_n = r_{n-2} - (r_{n-3} - r_{n-2} \cdot q_{n-1})q_n = \ldots.$$

(идем по цепочке равенств снизу вверх, выражая из каждого следующего равенства остаток и подставляя его в получившееся уже к этому моменту выражение)

$$\cdots = a \cdot r + b \cdot s = \text{НОД}(s, r).$$

Фактически мы доказали, что для любых двух целых чисел НОД есть линейная комбинация этих чисел.

Пример. Ранее было найдено $(525,\ 231) = 21$. Линейное представление наибольшего общего делителя:

$$21 = 63 - 42 \cdot 1 = 63 - (231 - 63 \cdot 3) \cdot 1 =$$

$$= 525 - 231 \cdot 2 - (231 - (525 - 231 \cdot 2) \cdot 3) = 525 \cdot 4 - 231 \cdot 9,$$

$$(525,\ 231) = 525 \cdot 4 + 231 \cdot (-9).$$

"Обратный" ход алгоритма Евклида называют также расширенным вариантом алгоритма (РАЕ).

Практическое выполнение алгоритма Евклида "вручную" удобно выполнять на специальном бланке.

остатки	частные	a_i	b_i
525	—	0	1
231	—	1	0
63	2	-2	1
42	3	7	-3
21	1	-9	4
0	2		

Важное приложение РАЕ состоит в нахождении мультипликативных обратных элементов в поле классов вычетов $\mathbb{Z}_p$ или $\mathbb{GF}(p)$, p - простое . Если взять ненулевой элемент $0 < r < p$, то $(p,\ r) = 1$.

Используя РАЕ, получим a и b такие, что $a \cdot r + b \cdot p = 1$. В модульной арифметике будет $1 \equiv a \cdot r(\mod p) r^{-1} \equiv a(\mod p)$.

Пример. Найти в $\mathbb{GF}(37)$ 17^{-1}. Применим РАЕ, вычисления проводим на бланке.

остатки	частные	a_i	b_i
37	—	0	1
17	—	1	0
3	2	-2	1
2	5	11	-5
1	1	-13	6
0	1		

Ответ: $(37,\ 17) = 17 \cdot (-13) + 37 \cdot 6, \quad -13 \equiv 24 \mod 37 \Rightarrow 17^{-1} = 24.$

Алгоритм Евклида для многочленов

В кольце многочленов над некоторым полем алгоритм Евклида может быть использован для нахождения НОД многочленов $(r(x),\ s(x))$. РАЕ позволяет найти такие многочлены $a(x)$ и $b(x)$, что

$$(r(x),\ s(x)) = a(x)r(x) + b(x)s(x).$$

Если многочлены взаимно просты, т.е. $(r(x),\ s(x)) = 1$, то $a(x)$ будет мультипликативным обратным для $r(x)$ в кольце многочленов по модулю $\mod s(x)$. Пусть $s(x)$ неприводим над соответствующим полем. Тогда любой многочлен степени менее $\deg s(x)$ будет с ним взаимно простым. Значит для любого ненулевого многочлена из кольца по $\mod s(x)$ существует обратный. Следовательно, многочлены с арифметикой по модулю неприводимого многочлена образуют поле.

Пример. Найти многочлен $(x^3+x^2)^{-1}$ в $\mathbb{GF}(2)[x]/x^4+x+1$.

остатки	частные	a_i
x^4+x+1	—	0
x^3+x^2	—	1
x^2+x+1	$x+1$	$x+1$
x	x	x^2+x+1
1	$x+1$	x^3+x
0	x	

остатки	частные	a_i
11001	—	0
0011	—	1
111	11	11
01	01	11
1	11	0101
0	10	

Во второй табличке записаны векторы коэффициентов степеней многочлена в порядке возрастания.

Получаем $(x^3+x^2)^{-1} \equiv x^3+x \pmod{x^4+x+1}$.

Пример. Найти такой многочлен (F) в $\mathbb{GF}(7)[x]$ степени меньше 4, что

$$(x^2-1)F \equiv (x^3+2\cdot x+5) \pmod{x^4+2x^2+1}.$$

Надо найти мультипликативный обратный элемент x^2-1, поскольку умножив на него обе части сравнения мы изолируем F в левой части. Сделаем это с помощью алгоритма Евклида, начав с пары x^4+2x^2+1 и x^2-1:

$$x^4+2x^2+1 = (x^2-1)*(x^2+3)+4.$$

Поскольку в остатке константа (многочлен нулевой степени) мы можем выполнять обратный ход:

$$
\begin{aligned}
1 &= 2 * 4 \pmod 7 \\
&= 2 * [(x^4 + 2 * x^2 + 1) - (x^2 + 3) * (x^2 - 1)] \pmod 7, \\
&= 2 * (x^4 + 2 * x^2 + 1) - 2 * (x^2 + 3) * (x^2 - 1) \pmod 7, \\
&= 2 * (x^4 + 2 * x^2 + 1) + (5 * x^2 + 1) * (x^2 - 1) \pmod 7, \\
1 &= (5 * x^2 + 1) * (x^2 - 1) \pmod{x^4 + 2 * x^2 + 1, 7}.
\end{aligned}
$$

Это значит, что $5 * x^2 + 1$ есть мультипликативный обратный для $x^2 - 1$. Теперь умножим обе части исходного сравнения (это можно!) на $5 * x^2 + 1$ по модулю многочлена $x^4 + 2 * x^2 + 1$, вычисляя коэффициенты по модулю 7.

$-2*(x^2+3) = -2*x^2-6 = 5*x^2+1+7*(-x^2-1)$. После ограничения коэффициентов по модулю 7, последнее слагаемое обратится в нуль.

Пример. Рассмотрим неприводимый над GF(2) многочлен

$$f(x) = x^8 + x^6 + x^5 + x + 1.$$

Найдем в $\mathbb{GF}(2)[x]/(x^8+x^6+x^5+x+1)$ элемент обратный к x^4+1.

$$
\begin{aligned}
x^8 + x^6 + x^5 + x + 1 &= (x^4 + x^2 + x + 1) * (x^4 + 1) + (x^2), \\
x^4 + 1 &= (x^2) * (x^2) + 1
\end{aligned}
$$

и, выполняя обратный ход PAE,

$$
\begin{aligned}
1 &= 1 * (x^4 + 1) + (x^2) * (x^2) \\
&= 1 * (x^4 + 1) + (x^2) * ([x^4 + x^2 + x + 1] * [x^4 + 1] + [x^8 + x^6 + x^5 + x + 1]) \\
&= (x^6 + x^4 + x^3 + x^2 + 1) * (x^4 + 1) + (x^2) * (x^8 + x^6 + x^5 + x + 1)
\end{aligned}
$$

что по модулю $f(x)$, дает

$$1 = (x^6 + x^4 + x^3 + x^2 + 1) * (x^4 + 1)(\mod f(x)).$$

Таким образом, искомый мультипликативный обратный элемент $(x^4 + 1)^{-1} = x^6 + x^4 + x^3 + x^2 + 1$.

Вычисления можно оформить на бланке.

остатки	частные	a_i
$x^8 + x^6 + x^5 + x + 1$	—	0
$x^4 + 1$	—	1
x^2	$x^4 + x^2 + x + 1$	$x^4 + x^2 + x + 1$
1	x^2	$x^6 + x^4 + x^3 + x^2 + 1$
0	x^2	