1 Алгоритм Евклида и его сложность

Определение 1. *Общим делителем* чисел a и b называется такое число c, что $c|a$ и $c|b$.

Определение 2. *Наибольшим общим делителем* чисел a и b называется такой их общий делитель, который делится на любой другой их общий делитель. Обозначается НОД(a, b) или (a, b).

Определение 3. *Общим кратным* чисел a и b называется такое число c, что $a|c$ и $b|c$.

Определение 4. *Наименьшим общим кратным* чисел a и b называется такое их общее кратное, который делит любое другое их общее кратное. Обозначается НОК(a, b) или $[a, b]$.

Пусть $a, b \in \mathbb{Z}$ — целые ненулевые числа. Известно, что существует единственный способ представить их в виде произведения простых чисел.

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

будем предполагать, что некоторые из α_i, β_i могут быть нулевыми. Несложно понять, что

$$\text{НОД}(a, b) = p_1^{\min(\alpha_1,\beta_1)} \dots p_k^{\min(\alpha_k,\beta_k)}$$
$$\text{НОК}(a, b) = p_1^{\max(\alpha_1,\beta_1)} \dots p_k^{\max(\alpha_k,\beta_k)}$$

Однако этот способ нахождения НОД очень трудоемкий из-за необходимости раскладывать a и b на множители. Рассмотрим другой способ нахождения НОД.

Пусть $a, b \in \mathbb{Z}$ — целые ненулевые числа, тогда существует единственная пара целых чисел q, r такая, что $a = bq + r$, причем $0 \le r < |b|$. Пусть c – общий делитель a и b. Тогда $c|r$. На основе этого несложного утверждения можно построить следующий алгоритм нахождения НОД.

Алгоритм 1 (Алгоритм Евклида)**.** *Пусть даны* $a, b \in \mathbb{Z}$.

1. *Разделим* a *на* b *с остатком* $a = bp_1 + q_1$.
2. *Разделим* b *на* q_1 *с остатком* $b = q_1 p_2 + q_2$.
3. *Продолжаем делить делитель на остаток* $q_i = q_{i+1} p_{i+2} + q_{i+2}$.
4. *Предпоследний шаг* $q_k = q_{k+1} p_{k+2} + q_{k+2}$.
5. *И на последнем шаге разделилось нацело* $q_{k+1} = q_{k+2} p_{k+3}$.

Утверждение 1. *Алгоритм Евклида конечен и* $q_{k+2} = НОД(a, b)$.

Доказательство. Покажем, что алгоритм Евклида конечен. Из определения деления с остатком имеем

$$|b| > |q_1| > |q_2| > \dots > |q_{k+2}|.$$

Т.е. модуль остатка постоянно уменьшается. Но он не может быть меньше 0. Следовательно, на некотором шаге он станет равен 0. Это и будет последний шаг.

Покажем, что $q_{k+2} = \text{НОД}(a, b)$. Сначала покажем, что это их общий делитель. Рассмотрим последний шаг $q_{k+1} = q_{k+2} p_{k+3}$. Из него следует, что $q_{k+2}|q_{k+1}$. Рассмотрим предпоследний шаг $q_k = q_{k+1} p_{k+2} + q_{k+2}$. Из него следует, что $q_{k+2}|q_k$. И так далее. Получаем, что $q_{k+2}|a$ и $q_{k+2}|b$.

Теперь покажем, что любой общий делитель a и b делит q_{k+2}. Пусть c это некоторый общий делитель a и b. Тогда из первого шага следует, что $c|q_1$. Тогда из второго шага следует, что $c|q_2$. И так далее. Получаем, что $c|q_{k+2}$. □

Пример 1.1. *Найти наибольший общий делитель* 144 *и* 80.

$$\begin{aligned} 144 &= 80 \cdot 1 + 64 \\ 80 &= 64 \cdot 1 + 16 \\ 64 &= 16 \cdot 4 \end{aligned}$$

Таким образом $НОД(144, 80) = 16$.

Существует модификация алгоритма Евклида. Если на каждом шаге осуществляется деление с остатком $a = bq + r$ так, что $-|b|/2 \leq r < |b|/2$, то говорят, что применяется алгоритм Евклида с выбором наименьшего по модулю остатка.

Пример 1.2. *Найти наибольший общий делитель* 144 *и* 80.

$$\begin{aligned} 144 &= 80 \cdot 2 - 16 \\ 80 &= 16 \cdot 5 \end{aligned}$$

Таким образом НОД$(144, 80) = 16$.

С помощью алгоритма Евклида наибольший общий делитель чисел a и b можно представить в виде линейной комбинации этих чисел, а именно, существуют целые числа x_0, y_0 такие, что $x_0a + y_0b = \text{НОД}(a, b)$. Такое представление называется линейным разложением наибольшего общего делителя чисел a, b. Приведем алгоритм нахождения разложения для двух чисел.

Алгоритм 2 (Нахождение линейного разложения)**.** *Пусть даны* $a, b \in \mathbb{Z}$.

1. *Выпишем деления с остатком, получающиеся из алгоритма Евклида*

$$\begin{aligned} a &= bp_1 + q_1 \\ b &= q_1p_2 + q_2 \\ q_1 &= q_2p_3 + q_3 \\ &\dots \\ q_k &= q_{k+1}p_{k+2} + q_{k+2}. \end{aligned}$$

   Пусть на следующем шаге разделится нацело.

2. *Из последнего уравнения выразим*

$$q_{k+2} = q_k - q_{k+1}p_{k+2}. \tag{1}$$

3. *Из предпоследнего равенства выразим* $q_{k+1} = q_{k-1} - q_kp_{k+1}$. *И подставим в (1).*

4. *Повторяем предыдущий шаг.*

5. *Получаем выражение вида* $ax_0 + by_0 = q_{k+1}$.

Пример 1.3. *Найти линейное разложение наибольшего общего делителя* 144 *и* 80. *Выпишем равенства, получаемые из алгоритма Евклида*

$$\begin{aligned} 144 &= 80 \cdot 1 + 64 \\ 80 &= 64 \cdot 1 + 16 \end{aligned}$$

Имеем

$$16 = 80 - 64 \cdot 1$$

Выражаем $64 = 144 - 80 \cdot 1$. *И подставляем в предыдущее равенство*

$$16 = 80 - 64 \cdot 1 = 80 - (144 - 80 \cdot 1) \cdot 1 = 80 \cdot 2 - 144$$

Таким образом мы нашли линейное разложение $16 = 80 \cdot 2 - 144$.

Замечание 1. Вышеизложенные результаты несложно переносятся на произвольное количество чисел.

1.1 Сложность алгоритма Евклида

Лемма 1 (Ламе)**.** *Рассмотрим остатки, получаемые в процессе деления в алгоритме Евклида. Для них выполнено* $r_{j+2} < r_j/2$.

Доказательство. Если $r_{j+1} \le r_j/2$, то сразу получаем, что $r_{j+2} < r_{j+1} \le r_j/2$. Пусть теперь $r_{j+1} > r_j/2$. В этом случае следующее деление дает $r_j = 1 \cdot r_{j+1} + r_{j+2}$ и $r_{j+2} = r_j - r_{j+1} < r_j/2$. □

Так как за каждые два шага остаток уменьшается, по крайней мере вдвое и так как остаток не может стать меньше 1, то производится не более $2[\log a]$ делений. Из данной леммы вытекает, что наихудший случай для алгоритма Евклида это два последовательных числа Фибоначчи.

Сам-о!. *Найдите наихудший случай для обобщенного алгоритма Евклида*

2 Сравнения по модулю. Теоремы Ферма и Эйлера

Определение 5. Пусть $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Говорят, что a *сравнимо* с b по модулю m, если $(a - b)$ делится на m. В этом случае будем писать $a \equiv b (\mathrm{mod}\ m)$.

Основные свойства сравнений:

1. $a \equiv a (\mathrm{mod}\ m)$;
2. $a \equiv b (\mathrm{mod}\ m) \Rightarrow b \equiv a (\mathrm{mod}\ m)$;
3. $a \equiv b (\mathrm{mod}\ m),\ b \equiv c (\mathrm{mod}\ m) \Rightarrow a \equiv c (\mathrm{mod}\ m)$;
4. $a \equiv b (\mathrm{mod}\ m) \Rightarrow ca \equiv cb (\mathrm{mod}\ m)$;
5. $ca \equiv cb,\ (c, m) = 1 \Rightarrow a \equiv b (\mathrm{mod}\ m)$;
6. $a \equiv b (\mathrm{mod}\ m) \Rightarrow ca \equiv cb (\mathrm{mod}\ cm)$;
7. $a \equiv b (\mathrm{mod}\ m),\ c \equiv d (\mathrm{mod}\ m) \Rightarrow a \pm c \equiv b \pm d (\mathrm{mod}\ m)$;
8. $a \equiv b (\mathrm{mod}\ m) \Rightarrow a^n \equiv b^n (\mathrm{mod}\ m)$;
9. $a \equiv b (\mathrm{mod}\ m),\ f(x)$ – многочлен с целыми коэффициентами $\Rightarrow f(a) \equiv f(b) (\mathrm{mod}\ m)$
10. $a \equiv b (\mathrm{mod}\ m_1), \ldots, a \equiv b (\mathrm{mod}\ m_k) \Rightarrow a \equiv b (\mathrm{mod}\ \mathrm{НОК}(m_1, \ldots, m_k))$;
11. $a \equiv b (\mathrm{mod}\ m),\ d | m \Rightarrow a \equiv b (\mathrm{mod}\ d)$;
12. $a^k \equiv b^k (\mathrm{mod}\ m),\ k | n \Rightarrow a^n \equiv b^n (\mathrm{mod}\ m)$.

Рассмотрим следующее *линейное сравнение* $ax \equiv b (\mathrm{mod}\ m)$. Его можно переписать в виде $m | (ax - b)$. Или в виде *диофантового уравнения* $ax - my = b$.

Рассмотрим диофантово уравнение вида $ax + by = m$. Было доказано, что существуют такие x_0, y_0, что $ax_0 + by_0 = \mathrm{НОД}(a, b)$. Следовательно уравнение $ax + by = m$ разрешимо тогда и только тогда, когда $\mathrm{НОД}(a, b) | m$. Одно из решений этого уравнения можно найти следующим образом

$$x_1 = \frac{x_0 m}{\mathrm{НОД}(a, b)} \qquad y_1 = \frac{y_0 m}{\mathrm{НОД}(a, b)}$$

Тогда множество всех решений имеет вид

$$\left\{ x_1 + \frac{tb}{\mathrm{НОД}(a, b)} : t \in \mathbb{Z} \right\} \qquad \left\{ y_1 - \frac{ta}{\mathrm{НОД}(a, b)} : t \in \mathbb{Z} \right\}$$

Перепишем теперь полученный результат в терминах линейного сравнения $ax \equiv b (\mathrm{mod}\ m)$. Получим, что если x_0 это одно из решений сравнения, то множество всех решений имеет вид

$$\left\{ x_1 + \frac{tb}{\mathrm{НОД}(a, b)} : t \in \mathbb{Z} \right\} \Leftrightarrow x \equiv x_0 \left(\mathrm{mod}\ \frac{m}{\mathrm{НОД}(a, m)} \right)$$

Пусть m – натуральное число, большее 1. Количество натуральных чисел, меньших m, которые взаимнопросты с m, обозначим $\varphi(m)$. Функция φ называется функцией Эйлера.

Теорема 1. *Функция Эйлера мультипликативна, т.е.*

$$\varphi(mn) = \varphi(n)\varphi(m)$$

для взаимнопростых m, n.

Доказательство. Пусть a пробегает все числа меньше m и взаимнопростые с ним. А b пробегает все числа меньше n и взаимнопростые с ним.

Покажем, что среди чисел вида $an + bm$ нет сравнимых по модулю mn. Пусть это не так. Тогда

$$a_1 n + b_1 m \equiv a_2 n + b_2 m (\text{mod } mn)$$

По свойствам сравнений можно записать

$$a_1 n \equiv a_2 n (\text{mod } m) \Leftrightarrow a_1 \equiv a_2 (\text{mod } m)$$
$$b_2 m \equiv b_2 m (\text{mod } n) \Leftrightarrow b_1 \equiv b_2 (\text{mod } m)$$

Получили противоречие.

Покажем, что НОД$(an + bm, mn) = 1$. Пусть это не так. Не нарушая общности, предположим, что $q|m$ и $q|(an + bm)$. Тогда $q|an$, но НОД$(m, n) = 1$, следовательно $q|a$. Противоречие с условием $(a, m) = 1$.

Теперь покажем, что $an + bm$ пробегает все числа меньше mn и взаимнопростые с ним.

$$\text{НОД}(an + bm, nm) = 1 \Leftrightarrow$$
$$\text{НОД}(an + bm, m) = 1,\ \text{НОД}(an + bm, n) = 1 \Leftrightarrow$$
$$\text{НОД}(a, m) = 1,\ \text{НОД}(b, n) = 1$$

Следовательно, существует ровно $\varphi(n)\varphi(m)$ чисел меньших mn и взаимнопростых с ним. Т.е. получаем

$$\varphi(mn) = \varphi(n)\varphi(m)$$

□

Утверждение 2. *Для простого* p *и натурального* k *выполнено*

$$\varphi(p) = p - 1$$
$$\varphi(p^k) = p^k - p^{k-1}$$

Из вышеизложенного получаем.

Утверждение 3. *Для произвольных простых* p_i *и целых неотрицательных* α_i *выполнено*

$$\varphi(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = p_1^{\alpha_1} \dots p_k^{\alpha_k}(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k})$$

Теорема 2 (Теорема Ферма)**.** *Для любого* m *и простого* p *таких, что НОД*$(p, m) = 1$ *выполнено*

$$a^{p-1} \equiv 1 (mod\ m)$$

Теорема 3 (Теорема Эйлера)**.** *Для любых* a, m *таких, что НОД*$(a, m) = 1$ *выполнено*

$$a^{\varphi(m)} \equiv 1 (mod\ m)$$

3 Великая китайская теорема об остатках. Решение систем линейных сравнений

Пусть $m_1, m_2, \dots, m_k$ - попарно взаимнопростые натуральные числа и $m = m_1 m_2 \dots m_k$, а $c_1, c_2, \dots, c_k$ - целые числа.

Теорема 4 (Великая китайская теорема об остатках)**.** *Множество решений системы линейных сравнений*

$$\begin{cases} x \equiv & c_1 (mod\ m_1) \\ x \equiv & c_2 (mod\ m_2) \\ \dots & \\ x \equiv & c_k (mod\ m_k) \end{cases}$$

имеет вид

$$x \equiv c_1 x_1 \frac{m}{m_1} + \dots + c_k x_k \frac{m}{m_k}$$

где $x_i \frac{m}{m_i} \equiv 1 (mod\ m_i)$.

Пример 3.1. *Решите систему сравнений*

$$\begin{cases} 7x \equiv \ \ 11(mod\ 18) \\ 8x \equiv \ \ \ 1(mod\ 27) \\ 9x \equiv \ \ 13(mod\ 28) \end{cases}$$

Преобразуем исходную систему. Разобьем каждое из сравнений на сравнения по примарным модулям. Получим

$$\begin{cases} 7x \equiv 11(mod\ 2),\ 7x \equiv 11(mod\ 3^2) \\ 9x \equiv 13(mod\ 2^2),\ 9x \equiv 13(mod\ 7) \\ \qquad\qquad\qquad\qquad 8x \equiv 1(mod\ 3^3) \end{cases}$$

Решаем каждое из этих сравнений. Получаем

$$\begin{cases} \ \ x \equiv 3(mod\ 7) \\ x \equiv 17(mod\ 3^3) \\ \ \ x \equiv 1(mod\ 2^2) \end{cases}$$

Применяем великую китайскую теорему об остатках. Необходимо решить следующую систему сравнений

$$\begin{cases} 108x_1 \equiv 1(mod\ 7) \\ 28x_2 \equiv 1(mod\ 27) \\ 189x_3 \equiv 1(mod\ 4) \end{cases}$$

Решаем и получаем $x_1 = 5$, $x_2 = 1$, $x_3 = 1$. *Записываем решение исходной системы*

$$x \equiv 3 \cdot 5 \cdot 27 \cdot 4 + 17 \cdot 1 \cdot 7 \cdot 4 + 1 \cdot 1 \cdot 7 \cdot 27 \equiv 17(mod\ 756)$$

Пример 3.2. *Используя теорему Эйлера и великую китайскую теорему об остатках, найдите остаток при длении* $8 \cdot 5^{41}$ *на* 96.
Пусть $x \equiv 8 \cdot 5^{41}(mod\ 2^5 \cdot 3)$, *тогда*

$$\begin{cases} x \equiv 8 \cdot 5^{41}(mod\ 2^5) \\ \ \ x \equiv 8 \cdot 5^{41}(mod\ 3) \end{cases}$$

Используя теорему Эйлера, находим, что

$$\begin{cases} x \equiv 8(mod\ 32) \\ \ \ x \equiv 1(mod\ 3) \end{cases}$$

Используя великую китайскую теорему об остатках, находим $x \equiv 40(mod\ 96)$.