Глава 3

УРАВНЕНИЯ И НЕРАВЕНСТВА. ЦЕЛОЧИСЛЕННАЯ МАТЕМАТИКА

§3.1. Уравнения n-й степени

3.1.1. Уравнение n-й степени. Исключение слагаемых $(n-1)$-й степени. Понижение степени уравнения с известным корнем (случай корня $x=0$ и общий случай). Разложение Виета для многочлена n-й степени с n корнями. В главе 1 приведен общий метод решения квадратных уравнений. Встречаются и более сложные уравнения n-й степени вида

$$P(x)=0, \tag{3.1}$$

содержащие *многочлен n-й степени* $P(x)$

$$P(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0.$$

Обсудим приемы, позволяющие в отдельных случаях упрощать уравнения n-й степени. Одним них является исключение слагаемого, пропорционального x^{n-1}.

Заменой $x=y-a_{n-1}/n$ уравнение (3.1) приводится к виду

$$\left(y-\frac{a_{n-1}}{n}\right)^n+a_{n-1}\left(y-\frac{a_{n-1}}{n}\right)^{n-1}+\ldots+a_0=0.$$

Раскрывая скобки, получаем, что слагаемые, пропорциональные y^{n-1}, сокращаются.

Если известен один корень уравнения (3.1), можно упростить уравнение, понизив его степень на единицу. Начнем со случая корня $x=0$.

Уравнение (3.1) имеет корень $x = 0$, только если $a_0 = 0$. В этом случае многочлен $P(x)$ распадается на произведение

$$P(x) = xQ(x), \quad \text{где } Q(x) = x^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1.$$

Ненулевые корни уравнения $P(x) = 0$ удовлетворяют уравнению меньшей степени $Q(x) = 0$.

Пусть теперь уравнение (3.1) имеет корень $x = x_0$.

Рассмотрим замену $x = x_0 + y$ в уравнении (3.1). Преобразованиие уравнение будет иметь корень $y = 0$; его левая часть поэтому будет распадаться на произведение $P(x) = yR(y)$, или

$$P(x) = (x - x_0)Q(x), \tag{3.2}$$

где $R(y)$ и $Q(x)$ — многочлены $(n-1)$-й степени.

Таким образом, другие (кроме $x = x_0$) корни уравнения $P(x) = 0$ являются решениями уравнения на единицу меньшей степени $Q(x) = 0$.

Если уравнение n-й степени $P(x) = 0$ имеет n известных корней $x = x_1$, …, $x = x_n$, можно понизить степень уравнения n раз, записав для многочлена n-й степени $P(x)$ разложение Виета:

$$P(x) = (x - x_1)\ldots(x - x_n). \tag{3.3}$$

3.1.2. Решение уравнений третьей степени (решение в радикалах, тригонометрический метод). Итальянскими математиками XVI века был предложен метод решения уравнений третьей и четвертой степени в радикалах. Начнем с обсуждения способа решения кубического уравнения общего вида. Исключая при необходимости слагаемое, пропорциональное x^2 (см. пункт 3.1.1), можно записать уравнение как

$$x^3 = 3px + 2q, \tag{3.4}$$

Идея метода решения уравнения (3.4) — представить корень уравнения в виде суммы

$$x = u + v$$

величин u и v, удовлетворяющих системе:

$$u^3 + v^3 = 2q, \qquad uv = p. \tag{3.5}$$

Действительно, если числа $(u; v)$ удовлетворяют системе (3.5), то

$$x^3 = (u+v)^3 = u^3 + 3uv(u+v) + v^3 = 3px + 2q.$$

Система уравнений (3.5) представляет из себя вавилонскую задачу (сумма чисел u^3 и v^3 равна $2q$, а произведение равно p^3) с известным решением

$$u = \sqrt[3]{q \pm \sqrt{q^2 - p^3}}\,, \qquad v = \sqrt[3]{q \mp \sqrt{q^2 - p^3}}\,,$$

существующим при

$$q^2 \geqslant p^3. \tag{3.6}$$

Отсюда находим один из корней уравнения (3.4):

$$x_0 = \sqrt[3]{q + \sqrt{q^2 - p^3}} + \sqrt[3]{q - \sqrt{q^2 - p^3}}\,, \tag{3.7}$$

понижая степень уравнения на единицу [1]).

Пусть теперь условие (3.6) не выполнено. В этом случае можно придать смысл соотношению (3.7), используя комплексные числа [2]). Чтобы обойтись без них, можно воспользоваться тригонометрическим методом Виета. Идея заключается в переходе от переменной x к переменной φ

$$x = A\cos\varphi \tag{3.8}$$

и подборе подходящего значения A. Для дальнейшего упрощения уравнения используется формула косинуса тройного угла.

---

[1]) Читателю предлагается самостоятельно установить, что при условии (3.6) других корней кубическое уравнение не имеет

[2]) Именно так комплексные числа впервые появились в математике

Сначала получим [1]) выражение для $\cos 3\varphi$. По формуле сложения,

$$\cos 3\varphi = \cos(2\varphi + \varphi) = \cos 2\varphi \cos \varphi - \sin 2\varphi \sin \varphi.$$

Обозначим $t = \cos \varphi$. Учтем, что $\cos 2\varphi = 2t^2 - 1$, а $\sin 2\varphi \sin \varphi = 2 \sin^2 \varphi \cos \varphi = 2t(1 - t^2)$. Тогда

$$\cos 3\varphi = (2t^2 - 1)t - 2t(1 - t^2) = 4t^3 - 3t.$$

Замена (3.8) приводит уравнение (3.4) к виду:

$$A^3 \cos^3 \varphi - 3pA \cos \varphi = 2q.$$

Чтобы воспользоваться формулой косинуса тройного угла, выберем $A = 2\sqrt{p}$: тогда уравнение

$$4 \cos^3 \varphi - 3 \cos \varphi = q/p^{3/2}$$

упрощается:

$$\cos 3\varphi = q/p^{3/2}. \tag{3.9}$$

Таким образом, корень уравнения (3.4) можно подобрать в виде $x = 2\sqrt{p} \cos \varphi$, где φ удовлетворяет соотношению (3.9). Поскольку косинус пробегает значения от -1 до 1, метод Виета применим только в случае $|q/p^{3/2}| \leqslant 1$, то есть в тех случаях, когда соотношение (3.6) не выполнено.

3.1.3. Решение уравнений четвертой степени. Рассмотрим уравнение четвертой степени, которое методом пункта 3.1.1 приводится к виду:

$$x^4 + b_2 x^2 + b_1 x + b_0 = 0. \tag{3.10}$$

Идея решения — в таком выборе параметра p, чтобы уравнение (3.10) приводилось к виду

$$(x^2 + p)^2 = a(x - b)^2. \tag{3.11}$$

Параметр p должен быть подобран таким образом, чтобы функция

$$R(x) = (x^2 + p)^2 - (x^4 + b_2 x^2 + b_1 x + b_0)$$

[1]) Виет обосновывал формулу для $\cos 3\varphi$ геометрически

представлялась в виде $R(x) = a(x-b)^2$. Выражение $R(x)$ является квадратным трехчленом

$$R(x) = (2p - b_2)x^2 - b_1 x + (p^2 - b_0),$$

который имеет ровно один корень, являясь полным квадратом, при

$$b_1^2 = 4(2p - b_2)(p^2 - b_0). \tag{3.12}$$

Таким образом, уравнение четвертой степени общего вида для x свелось к уже исследованному ранее уравнению третьей степени (3.12) для p.

§3.2. Специальные типы уравнений и неравенств

3.2.1. Методы решения уравнений и неравенств с модулями и радикалами (раскрытие модуля, замены, равносильные преобразования). Перечислим основные способы решений уравнений и неравенств вида

$$|f| \vee g, \qquad \sqrt{f} \vee g,$$

где f и g — содержащие неизвестную переменную x выражения, $\vee$ — один из знаков $=$, $<$, $>$, $\leqslant$, $\geqslant$.

Таблица 3.1. Равносильные преобразования для уравнений и неравенств с модулями

Уравнение или неравенство	**Равносильная система (совокупность)**
$\lvert f\rvert = g$	$\begin{cases} (f = g \text{ или } f = -g) \\ g \geqslant 0 \end{cases}$
$\lvert f\rvert > g$	$(f > g \text{ или } f < -g)$
$\lvert f\rvert < g$	$(-g < f \text{ и } f < g)$

Первый метод заключается в раскрытии модуля путем рассмотрении различных промежутков изменения переменной: $|f|$ заменяется на $+f$ при $f \geqslant 0$ и на $-f$ при $f < 0$.

Второй метод использует переобозначения: иногда удобно бывает принять $|f|$ или $\sqrt{f}$ в качестве новой переменной t, выразив g через t.

Еще один метод основан на равносильных преобразованиях, представленных в таблицах 3.1 и 3.2.

Интересно отметить, что уравнение (неравенство) с модулем $|f| \vee g$ можно свести к уравнению (неравенству) с радикалом $\sqrt{f^2} \vee g$ — именно поэтому методы решения оказываются похожими.

3.2.2. Методы решения уравнений с показательными и логарифмическими функциями (замена переменной, отбрасывание логарифмов и основания степени). Простейшим приемом решения уравнений и неравенств с показательными и логарифмическими функциями является замена переменной: используют переобозначения $2^x = y$, $\log_3 x = y$. Также используются равносильные преобразова-

Таблица 3.2. Равносильные преобразования для уравнений и неравенств с радикалами

Уравнение или неравенство	**Равносильная система (совокупность)**
$\sqrt{f} = g$	$\begin{cases} f = g^2 \\ g \geqslant 0 \end{cases}$
$\sqrt{f} > g$	$\left(\begin{cases} g \geqslant 0 \\ f > g^2 \end{cases} \text{ или } \begin{cases} g < 0 \\ f \geqslant 0 \end{cases} \right).$
$\sqrt{f} < g$	$\begin{cases} g \geqslant 0 \\ 0 \leqslant f < g^2 \end{cases}$

ния из таблицы 3.3. Следует иметь в виду, что выражение a^x обычно рассматриваются при положительных основаниях $a > 0$. Однако, если x принимает целочисленные значения, надо рассматривать также отрицательные a.

3.2.3. Методы решения тригонометрических уравнений ($\sin x = 0$, $\cos x = \cos a$, $\sin x = \sin a$, $\operatorname{tg} x = \operatorname{tg} a$). Рассмотрим простейшее, «базовое» тригонометрическое уравнение

$$\sin x = 0. \tag{3.13}$$

Его решения таковы: $x = 0, \pm\pi, \pm 2\pi, \ldots$ (или $x = \pi n$, n — целое).

Уравнение

$$\cos x = \cos a \tag{3.14}$$

Таблица 3.3. Равносильные преобразования для уравнений и неравенств с логарифмическими и показательными функциями

Уравнение или неравенство	**Равносильная система (совокупность)**
$\log_a b = \log_a c$	$\begin{cases} b = c, b > 0 \\ a > 0, a \neq 1 \end{cases}$
$\log_a b < \log_a c$	$\begin{cases} 0 < b < c \\ a > 1 \end{cases}$ или $\begin{cases} 0 < c < b \\ 0 < a < 1 \end{cases}$
$\begin{cases} a^x = a^y \\ a > 0 \end{cases}$	$\begin{cases} x = y \\ a > 0 \end{cases}$ или $\begin{cases} x \text{ и } y \text{ определены} \\ a = 1 \end{cases}$
$\begin{cases} a^x < a^y \\ a > 0 \end{cases}$	$\begin{cases} x < y \\ a > 1 \end{cases}$ или $\begin{cases} x > y \\ 0 < a < 1 \end{cases}$

сводится к (3.13).

Действительно, обозначим $x = \beta + \gamma$, $a = \beta - \gamma$ (это означает, что $\beta = (x + a)/2$, $\gamma = (x - a)/2$). Тогда по формулам сложения

$$\cos x - \cos a = \cos(\beta + \gamma) - \cos(\beta - \gamma) = -2 \sin \beta \sin \gamma.$$

Поэтому разность

$$\cos x - \cos a = -2 \sin \frac{x + a}{2} \sin \frac{x - a}{2}$$

обращается в нуль в двух случаях:

$$\sin \frac{x - a}{2} = 0 \quad \Longleftrightarrow \quad x = a + 2\pi n;$$

$$\sin \frac{x + a}{2} = 0 \quad \Longleftrightarrow \quad x = -a + 2\pi n.$$

Найденные корни уравнения (3.14) можно записать как

$$x = \pm a + 2\pi n.$$

Решим уравнение $\sin x = \sin a$.

Равенство, приводяшееся к виду $\cos(\pi/2 - x) = \cos(\pi/2 - a)$, выполняется в двух случаях:

$$\frac{\pi}{2} - x = \frac{\pi}{2} - a - 2\pi n \quad \Longleftrightarrow \quad x = a + 2\pi n;$$

$$\frac{\pi}{2} - x = -\left(\frac{\pi}{2} - a\right) - 2\pi n \quad \Longleftrightarrow \quad x = \pi - a + 2\pi n.$$

Решим уравнение $\operatorname{tg} x = \operatorname{tg} a$.

Поскольку

$$\operatorname{tg} x - \operatorname{tg} a = \frac{\sin x \cos a - \cos x \sin a}{\cos x \cos a} = \frac{\sin(x - a)}{\cos x \cos a},$$

равенство $\operatorname{tg} x = \operatorname{tg} a$ выполнено, если $\sin(x - a) = 0$ при дополнительном условии $\cos x \neq 0$. Это означает, что $x = a + \pi n$.

§3.3. Делимость натуральных чисел

Для исследования простейших уравнений в целых числах изучим свойства делимости натуральных чисел.

3.3.1. Признаки делимости на 2, 3, 5, 9 и 10. В простейших случаях определить, делится ли одно число на другое, можно при помощи признаков делимости. Пусть число m записано цифрами a_0, a_1, ..., a_n, считая справа:

$$m = 10^n a_n + ... + 10a_1 + a_0.$$

Покажем, что число m делится на 2, 5, или 10 тогда и только тогда, когда его последняя цифра делится на 2, 5 и 10 соответственно.

Для доказательства достаточно заметить, что разность числа и его последней цифры равна

$$m - a_0 = 10a_1 + 100a_2 + 1000a_3 + \ldots$$

и делится на 2, 5 и 10.

Установим, что число m делится на 3 или 9 тогда и только тогда, когда сумма его цифр делится на 3 или 9 соответственно.

Для доказательство достаточно заметить, что разность числа и суммы его цифр:

$$m - (a_0 + a_1 + \ldots + a_n) = 9a_1 + 99a_2 + \ldots + (10^n - 1)a_n.$$

делится на 3 и 9 (число $10^n - 1$ состоит из одних девяток).

3.3.2. Наибольший общий делитель двух чисел (два определения). Расчет наибольшего общего делителя методом Евклида. Пусть p_1 и p_2 — два натуральных числа. Натуральное число p называется *общим делителем* чисел p_1 и p_2, если p_1 и p_2 делятся на p. Среди всех общих делителей чисел p_1 и p_2 можно выделить *наибольший общий делитель* НОД(p_1, p_2).

Другое определение: наибольшим общим делителем чисел p_1 и p_2 называют наименьшее из натуральных чисел $r_{\min}(p_1, p_2)$, которые могут быть получены из чисел чисел

p_1 и p_2 применением операций сложения и вычитания:

$$r = (p_1 + ... + p_1) - (p_2 + ... + p_2) = k_1 p_1 - k_2 p_2$$

с некоторыми коэффициентами k_1 и k_2.

Рассмотрим в качестве примера наибольший общий делитель чисел 4 и 6. Осуществляя перебор всех чисел, находим, что по первому определению НОД$(4,6) = 2$. Чтобы воспользоваться вторым определением, заметим, что в виде $(4 + 4 + ... + 4) - (6 + 6 + ... + 6)$ могут быть представлены числа 0, ± 2 $(2 = 4 + 4 - 6)$, ± 4 и т.д. Из этих чисел натуральными являются 2, 4, 6, ... — наименьшее равно 2. Следовательно, $r_{\min}(4,6) = 2$.

Как для расчета НОД(p_1, p_2), так и для расчета $r_{\min}(p_1, p_2)$ можно использовать *алгоритм Евклида*, заключающийся в следующем. Записывается равенство

$$\text{НОД}(p_1, p_2) = \begin{cases} \text{НОД}(p_1 - p_2, p_2), & p_1 > p_2, \\ \text{НОД}(p_1, p_2 - p_1), & p_1 < p_2, \\ p_1, & p_1 = p_2. \end{cases}$$

Используя его конечное число раз, на некотором шаге приходим к ответу для НОД(p_1, p_2). Число шагов не может быть больше $p_1 + p_2$, так как на каждом шаге сумма чисел, наибольший делитель которых ищется, уменьшается.

Обоснование алгоритма вытекает из следующих утверждений:

- НОД$(p, p) = p$ (число p делится на p и не может делиться на большее число);
- НОД$(p, q) =$ НОД$(p - q, q)$ при $p > q$ (всякий общий делитель чисел p и q является общим делителем чисел $p - q$ и q, и наоборот);
- $r_{\min}(p, p) = p$ (в виде $p(k_1 - k_2)$ можно представить числа 0, $\pm p$, $\pm 2p$, ...);
- $r_{\min}(p, q) = r_{\min}(p - q, q)$ при $p > q$ (вытекает из свойства $pk_1 - qk_2 = (p - q)k_1 - q(k_2 - k_1)$).

Поскольку величины НОД(p_1, p_2) и $r_{\min}(p_1, p_2)$ рассчитываются одним и тем же способом, они равны:

$$\text{НОД}(p_1, p_2) = r_{\min}(p_1, p_2). \tag{3.15}$$

Отметим, что процедуру нахождения наибольшего общего делителя двух чисел можно ускорить, если проходить несколько шагов за один. Действительно, при $p_1 > np_2$ можно вместо $\text{НОД}(p_1, p_2) = \text{НОД}(p_1 - p_2, p_2)$ записать $\text{НОД}(p_1, p_2) = \text{НОД}(p_1 - np_2, p_2)$, а при $p_1 = np_2$ — писать $\text{НОД}(np_2, p_2) = p_2$. В этом случае шаг цепочки равенств оказывается следующим:

- если число $p_1 > p_2$ делится на p_2 с остатком r_1, то $\text{НОД}(p_1, p_2)$ заменяется на $\text{НОД}(r_1, p_2)$;
- если число $p_2 > p_1$ делится на p_1 с остатком r_2, то $\text{НОД}(p_1, p_2)$ заменяется на $\text{НОД}(p_1, r_2)$;
- если число p_1 делится на p_2 без остатка, то $\text{НОД}(p_1, p_2) = p_2$ — вычисление закончено;
- если число p_2 делится на p_1 без остатка, то $\text{НОД}(p_1, p_2) = p_1$ — вычисление закончено.

3.3.3. Взаимно простые числа. Достаточное условие взаимной простоты чисел p_1p_2 и q. Взаимная простота чисел $m/\text{НОД}(m,n)$ и $n/\text{НОД}(m,n)$. Два числа p_1 и p_2 называют *взаимно простыми*, если они не имеют общих делителей, кроме единицы. Как вытекает из второго определения наибольшего общего делителя, числа p_1 и p_2 взаимно просты тогда и только тогда, когда единицу можно представить в виде разности k_1 чисел p_1 и k_2 чисел p_2:

$$1 = k_1p_1 - k_2p_2 \quad \Longleftrightarrow \quad p_1 \text{ и } p_2 \text{ взаимно просты.}$$

Пусть числа p_1 и p_2 взаимно просты, числа p_1 и p_3 взаимно просты. Тогда числа p_1 и p_2p_3 взаимно просты.

Из условия вытекает, что для некоторых натуральных k_1, k_2, l_1 и l_2 справедливы свойства

$$k_1p_1 = k_2p_2 + 1, \quad l_3p_3 = l_1p_1 + 1.$$

Умножая первое равенство на l_3p_3, получим:

$$k_1p_1l_3p_3 = k_2l_3p_2p_3 + l_1p_1 + 1,$$

или

$$(k_1l_3p_3 - l_1)p_1 = k_2l_3p_2p_3 + 1.$$

Следовательно, числа p_1 и p_2p_3 взаимно просты.

Пусть m и n — два натуральных числа. Покажем, что числа $m/\text{НОД}(m,n)$ и $n/\text{НОД}(m,n)$ взаимно просты.

Предположим противное: пусть данные числа имеют общий делитель k, больший единицы. Тогда m и n делятся на $k\text{НОД}(m,n) > \text{НОД}(m,n)$, что противоречит определению наибольшего общего делителя.

3.3.4. Решение уравнения $Ax = By$ с неизвестными x и y в целых числах. Рассмотрим простейшее уравнение в целых числах

$$Ax = By \tag{3.16}$$

с неизвестными целыми числами x и y и известными параметрами A и B. Сначала рассмотрим случай, когда

$$\text{НОД}(A,B) = 1. \tag{3.17}$$

Поскольку случай $(x = 0; y = 0)$ тривиален, будем искать ненулевые решения уравнения (3.16). Пусть $r = \text{НОД}(|x|,|B|)$. Тогда для целых x_1 и B_1

$$x = rx_1, \quad B = rB_1, \quad \text{НОД}(x_1, B_1) = 1, \tag{3.18}$$

и уравнение (3.16) принимает вид

$$Ax_1 = B_1 y$$

При этом всякий общий делитель q чисел $|A|$ и $|B_1|$ является общим делителем чисел $|A|$ и $|B|$ — ввиду (3.17) $q = 1$.

Поскольку $|A|$ и $|B_1|$ взаимно просты, $|x_1|$ и $|B_1|$ взаимно просты, числа $|Ax_1| = |B_1 y|$ и $|B_1|$ также взамно просты. Поэтому $|B_1| = 1$. Из (3.18) получаем, что $r = |B|$ и $x = Bk$, где k целое.

Таким образом, наиболее общий вид решения уравнения (3.16) следующий:

$$x = Bk, \quad y = Ak, \quad k = 0, \pm 1, \pm 2, \ldots$$

Если числа A и B не являются взаимно простыми, уравнение следует разделить на $\text{НОД}(A,B)$ и свести к уже рассмотренному случаю. Если одно из чисел A и

B отрицательно, то уравнение сводится к исследованному случаю заменой $x = -z$.

3.3.5. Уравнение $Ax = By + C$: условие разрешимости, метод решения. Рассмотрим уравнение

$$Ax = By + C \tag{3.19}$$

с неизвестными целыми x и y. Обозначая $r = \text{НОД}(|A|, |B|)$, запишем:

$$A = rA_1, \quad B = rB_1, \quad \text{НОД}(A_1, B_1) = 1 \tag{3.20}$$

и преобразуем уравнение (3.19) к виду:

$$A_1x - B_1y = C/r. \tag{3.21}$$

Поскольку для взаимно простых чисел A_1 и B_1 всякое целое число можно представить в виде $A_1x - B_1y$, уравнения (3.21) и (3.19) разрешимы тогда и только тогда, когда C/r целое (C делится на $\text{НОД}(|A|, |B|)$).

Подобрав одну пару чисел $x = x_0$, $y = y_0$, удовлетворяющую уравнению (3.19), можно построить и все остальные решения.

Вычитая из уравнения (3.19) соотношение $Ax_0 = By_0 + C$, приводим его к виду уже рассмотренного уравнения (3.16):

$$A(x - x_0) = B(y - y_0).$$

§3.4. Разложение на простые множители

3.4.1. Простые числа. Составление таблицы простых чисел (метод Эратосфена). Число p называется *простым*, если оно имеет только два делителя: единицу и p. Единица не относится к простым числам. Как вытекает из определения, два различных простых числа взаимно просты.

Для составления таблицы простых чисел Эратосфен в III веке до нашей эры предложил следующий алгоритм. В таблицу выписываются все числа из заданного промежутка в таблицу. Из нее сначала вычеркиваются числа, представимые в виде произведений $2 \cdot 3$, $2 \cdot 4$, ..., затем — в виде

произведений $3 \cdot 3$, $3 \cdot 5$, ... Незачеркнутыми остаются числа, не представимые в виде произвдений чисел, отличных от единицы и являющиеся простыми.

3.4.2. Метод нахождения простого делителя у числа. Возможность разложения числа на простые множители. Бесконечность множества простых чисел. У любого числа m найдется хотя бы один простой делитель. Его можно найти путем последовательного перебора чисел 2, 3, 4, 5, ... Первое из чисел p, на которое разделится m, будет простым делителем этого числа.

Предположим, что число p составное: $p = q_1 q_2$. Тогда в процессе перебора мы должны были учесть числа q_1 и q_2, на которые должно было разделиться m. Противоречие.

Подобрав простой делитель p_1 числа m, можно представить это число в виде $m = p_1 m_1$. Далее следует найти простой делитель p_2 числа m_1, записав $m_1 = p_2 m_2$. На каком-то i-м шаге ($i \leqslant m$) мы добьемся, чтобы $m_i = 1$. Тогда число m представится в виде *разложения на простые множители* $m = p_1 p_2 ... p_i$.

Как показал Евклид, множество простых чисел бесконечно.

Предположим, что имеется всего s простых чисел $p_1, ..., p_s$; тогда рассмотрим число $p = p_1 ... p_s + 1$, которое не делится ни на одно из простых чисел, и придем к противоречию.

3.4.3. Делимость чисел и разложение на простые множители. Пусть два числа представлены в виде произведения простых множителей $M = p_1^{m_1} p_2^{m_2} ... p_s^{m_s}$ и $N = p_1^{n_1} p_2^{n_2} ... p_s^{n_s}$. Установим, что M делится на N тогда и только тогда, когда $m_1 \geqslant n_1$, $m_2 \geqslant n_2$, ..., $m_s \geqslant n_s$.

Действительно, при $m_i \geqslant n_i$ имеем:

$$p_1^{m_1} ... p_s^{m_s} = p_1^{n_1} ... p_s^{n_s} \cdot p_1^{m_1 - n_1} ... p_s^{m_s - n_s},$$

и $p_1^{m_1} ... p_s^{m_s}$ делится на $p_1^{n_1} ... p_s^{n_s}$.

Обратно, предположим, что M делится на N:

$$p_1^{m_1} ... p_s^{m_s} = p_1^{n_1} ... p_s^{n_s} m.$$

Предположим, что $m_i < n_i$ для хотя бы одного i. Пусть для определенности $i = 1$. Тогда

$$p_2^{m_2}...p_s^{m_s} = p_1^{n_1-m_1}p_2^{n_2}...p_s^{n_s}m.$$

Следовательно, $p_2^{m_2}...p_s^{m_s}$ делится на p_1. Поскольку число p_1 является взаимно простым с любым из чисел $p_2, ..., p_s$, оно взаимно простое с произведением любого количества данных чисел. НОД$(p_1, p_2^{m_2}...p_s^{m_s}) = 1$, и число $p_2^{m_2}...p_s^{m_s}$ не может делиться на p_1. Получено противоречие.

3.4.4. Единственность разложения числа на простые множители. Общие делители и общие кратные двух чисел. Расчет наибольшего общего делителя и наименьшего общего кратного. Покажем, что разложение числа на простые множители единственно.

Пусть одно и то же число удалось разложить двумя способами на простые множители: $p_1^{n_1}...p_s^{n_s} = p_1^{n_1'}...p_s^{n_s'}$. Тогда $p_1^{n_1}...p_s^{n_s}$ делится на $p_1^{n_1'}...p_s^{n_s'}$, а $p_1^{n_1}...p_s^{n_s}$ делится на $p_1^{n_1'}...p_s^{n_s'}$. Следовательно, при всех i справедливы свойства $n_i \geqslant n_i'$ и $n_i' \geqslant n_i$. Таким образом, $n_i = n_i'$.

Пусть два числа разложены на простые множители:

$$M = p_1^{m_1}p_2^{m_2}...p_s^{m_s}, \qquad N = p_1^{n_1}p_2^{n_2}...p_s^{n_s}.$$

Все общие делители L этих чисел записываются в виде

$$L = p_1^{l_1}...p_s^{l_s}, \text{ где } l_i \leqslant m_i,\ l_i \leqslant n_i,$$

а все общие кратные K (числа, делящиеся и на M, и на N) — в виде

$$K = p_1^{k_1}...p_s^{k_s}p_{s+1}^{k_{s+1}}...p_q^{k_q}, \text{ где } l_i \geqslant m_i,\ l_i \geqslant n_i.$$

Здесь $p_{s+1}, ..., p_q$ — простые числа, отличные от $p_1, ..., p_s$.

Отметим, что общий делитель оказывается наибольшим при $l_i = \min(m_i, n_i)$, а общее кратное — наименьшим при $q = s,\ k_i = \max(m_i, n_i)$.