Югорский
физико-математический лицей

В.П. Чуваков

ОСНОВЫ ТЕОРИИ ЧИСЕЛ

Конспект лекций

$$n \equiv (n_0 + n_1 + n_2 + ... + n_k) \pmod 3$$

$$n \equiv (n_0 - n_1 + n_2 - n_3 + ...) \pmod{11}$$

Натуральные числа

$N=\{1,2,3,4,....,n,...\}$- множество натуральных чисел, используемых для счета или перечисления.

Система аксиом Пеано

1. Единица 1- натуральное число, которое не следует ни за каким числом.
2. Для любого натурального числа n существует единственное число n', которое непосредственно следует за n.
3. Каждое натуральное число $n\neq 1$ следует непосредственно лишь за одним числом.
4. Если некоторое множество M содержит 1 и вместе с каждым натуральным числом n содержит непосредственно следующее за ним число n', то $M=N$ (аксиома индукции).

Операции на множестве N.

Сложение

$$n+1=n';$$
$$n+m'=(n+m)'.$$

Умножение

$$n\cdot 1=n;$$
$$n\cdot m'=n\cdot m+n.$$

Свойства операций:

Ассоциативность: $n+(m+p)=(n+m)+p.$

Доказательство.

Пусть $M=\{p/n+(m+p)=(n+m)+p\}.$

Тогда $1\in M: n+m'=(n+m)'.$ Пусть $p\in M.$ Докажем, что $p'\in M.$ Действительно,

$n+(m+p')=n+(m+p)'=((n+(m+p))'=(n+m)+p'.$

Коммутативность: $n+m=m+n.$ *Доказательство.*

Пусть $M=\{p/\ p+1=1+p\}$. Тогда $1\in M$. Пусть $p\in M$.
Докажем, что $p'\in M$. Действительно,
$p'+1=(p+1)'=(1+p)'=1+p'$.
Пусть теперь $M=\{p/\ p+n=n+p\}$. Тогда $1\in M$. Пусть $p\in M$.
Докажем, что $p'\in M$. Действительно,
$n+p'=(n+p)'=(p+n)'=p+(n+1)=p+(1+n)=(p+1)+n$.
Следовательно, по аксиоме 4, $M=N$, т.е.
$\forall n,m: n+m=m+n$.

Дистрибутивность: $(m+p)\cdot n=m\cdot n+p\cdot n$.

Доказательство.
Пусть $M=\{p/(n+m)\cdot p=n\cdot p+m\cdot p\}$.
Тогда $1\in M: (n+m)\cdot 1=n+m$.
Пусть $p\in M$. Докажем, что $p'\in M$. Действительно,
$(n+m)\cdot p'=(n+m)p+(n+m)=np+mp+n+m=np'+m\,p'$.
Следовательно, по аксиоме 4, $M=N$.

Сравнение в N.

Определение: $n<m \Leftrightarrow \exists k$, такое, что $n+k=m$.

Утв.1 Для любых двух натуральных чисел n,m имеет место одно из трех соотношений: $m=n$; $m<n$; $m>n$.

Утв.2 Если $n<m$, $m<p$, то $n<p$.:

Утв.3 Если $n=m$, то $n+p=m+p$, $np=mp$.

Утв.4 Для любых натуральных чисел n,m,p. Если $n<m$, то $n+p<m+p$, $np<mp$.

Утв.5 Для любых натуральных чисел n,m существует натуральное число p, такое, что $n\cdot p>m$.

Вычитание: $a-b=c \Leftrightarrow a>b$, $b+c=a$.
Свойства вычитания: Если $a>c$, то $(a+b)-c=(a-c)+b$.
Если $b>c$, то $(a+b)-c=a+(b-c)$.

Некоторые особенности натуральных чисел:

1. Ни для какого натурального числа n не существует натурального числа p такого, что $n<p<n+1$.

2. Любое непустое подмножество натуральных чисел содержит наименьший элемент.

3. Если M – ограниченное сверху подмножество натуральных чисел $(\exists p, \forall x \in M, x<p)$, то в M существует наибольший элемент.

Принцип математической индукции

Если некоторое утверждение $P(n)$ справедливо для некоторых начальных $n=1,2,3,4....$ и из условия, что $P(k)$ справедливо для $n=k$, следует(удается доказать), что $P(k)$ справедливо для $n=k+1$, то это утверждение справедливо для любого n.

Пример 1. Докажите следующие утверждения методом математической индукции:

1) Справедливо тожество $1+2+3+...+n=\frac{n(n+1)}{2}$;

2) Справедливо тожество $1+2^2+3^2+...+n^2=\frac{n(n+1)(2n+1)}{6}$;

3) Справедливо тожество $1+3+5+...+2n-1=n^2$;

4) Выражение $4^n+15n-1$ делится на 9;

5) В любой момент времени число людей на земле, сделавших нечетное число рукопожатий, число четное;

6) Любое целое число рублей $n>7$ можно без сдать без сдачи только монетами по 3 и 5 рублей;

7) Если произведение положительных чисел $x_1 \cdot x_2 \cdot ... \cdot x_n = 1$, то $x_1+x_2+...+x_n \geq n$;

8) Плоскость, разделенную на области любым количеством прямых, можно раскрасить двумя красками так, что любые две соседние области будут иметь разный цвет.

9) При любом $n>1$ справедливо неравенство $(1+p)^n > 1+np.$

Делимость натуральных чисел

Деление: a делится на $b \Leftrightarrow \exists c$ такое, что $a = b \cdot c.$

Свойства операций:

1. Если $a_1, a_2, .., a_n$ делятся на b, то $a_1 + a_2 + .. + a_n$ делится на $b.$
2. Если $a > b$ и a, b делятся на c, то $a - b$ делится на $c.$
3. Если $a + b$ и b делятся на c, то a делится на $c.$
4. Если a делится на c, то $a \cdot b$ делится на $c.$
5. Если $a_1, a_2, ..., a_n$ делятся на b, а c не делятся на b, то то $a_1 + a_2 + ... + a_n + c$ не делится на $b.$
6. Если a или c делятся на b, то $a \cdot c$ делится на $b.$
7. Если a делится на bc, то a делится на b и a делится на $c.$

Теорема о делении с остатком Для любых натуральных чисел m, n существуют и единственные положительные числа t, p такие, что $n = m \cdot t + p,$ причем $p < m.$

Доказательство. Пусть $n > m.$ Рассмотрим следующий алгоритм:

$n - m = n_1;$ $n_1 - m = n_2;$ $n_2 - m = n_3;$ . . и т.д. $n_k - m = n_{k+1}.$	Если $n_1 > m$, то сделаем еще одно вычитание Если $n_2 > m$, то сделаем еще одно вычитание Продолжаем процесс вычитания до тех пор, пока остаток не будет меньше числа $m.$ Существует число k такое, что $n_{k+1} < m.$
$n - m \cdot (k+1) = n_{k+1}.$	Сложим все строки данного

	алгоритма и получим требуемое выражение, где $t=k+1,\ p=n_{k+1}$.

Единственность представления будем доказывать методом "от противного".

Предположим, что существует два представления $n=mk_1+p_1$ и $n=mk_2+p_2$. Вычтем одно выражение из другого $0=m(k_1-k_2)+p_1-p_2 \Rightarrow m(k_1-k_2)=p_2-p_1$, причем $p_1-p_2<m$. Последнее равенство в целых числах возможно только в случае $k_1-k_2=0,\ p_1-p_2=0$, так как $m(k_1-k_2)\geq m$ при $k_1-k_2\geq 0$. □

Приведенный в теореме 1 алгоритм отражает хорошо известную всем операцию деления натуральных чисел "столбиком".

Следствие 1. Всякое натуральное число можно представить в виде: $3m,\ 3m+1,\ 3m+2$ или $5p,5p+1,5p+2,5p+3,5p+4$ или $np,np+1,np+2,....,np+(n-1)$.

Следствие 2. Если $p_1,p_2,....,p_n-$ n подряд стоящих натуральных чисел, то одно из них делится на n.

Следствие 3. Если p_1,p_2- два последовательных четных числа, то одно из них делится на 4.

Определение. Натуральное число p называется простым, если оно не имеет делителей, кроме единицы и самого себя.

Следствие 4. Всякое простое число имеет вид $6p+1$ или $6p-1$.

Действительно, всякое число можно представить в виде $6p,6p+1,6p+2,6p+3,6p+4,6p+5$, однако все числа этого ряда, кроме $6p+1,6p+5$, точно являются составными. □

Следствие 5. Если $p\geq 5$ – простое число, то p^2-1 делится на 24.

Действительно, $p-1,\ p,\ p+1-$ три подрядстоящих натуральных числа, причем, $p-1,\ p+1-$четные, а $p-$ нечетное простое. Следовательно, одно из четных чисел $p-1$ и $p+1$ делится на 4, а одно – еще и на 3.□

Пример 2. Справедливы следующие утверждения:
1.Квадрат нечетного числа при делении на 8 дает остаток 1.
2. Ни при каком натуральном n число n^2+1 не делится на 3.
Доказательство1. Всякое нечетное число можно представить в виде $4p+1$ или $4p+3$. Возведем каждое из этих чисел в квадрат и получим требуемое утверждение.
Доказательство 2. Всякое натуральное число n можно представить в виде $3p, 3p+1, 3p+2$. Тогда выражение n^2+1 будет равно одному из выражений $9p^2+1$, $9p^2+6p+2$, $9p^2+18p+5$, которые не делятся на 3.

Пример 3. Решите в целых числах уравнение $n!-7k=1$
Решение. Если решение $n\geq 7$, то $n!$ делится на 7 и из уравнения следует, что 1 делится на 7. Следоваетельно при $n\geq 7$ решений нет. Тогда $n\leq 6$ и $n!=7k+1$. Переберем все числа от 1 до 6: $n=1: 1=7k+1 \Rightarrow k=0$; $n=2: 2=7k+1 \Rightarrow \varnothing$;
$n=3: 3!=6=7k+1 \Rightarrow \varnothing$; $n=4: 4!=24=7k+1 \Rightarrow \varnothing$;
$n=5: 5!=120=7k+1 \Rightarrow k=17$; $n=6: 6!=720=7k+1 \Rightarrow \varnothing$.
Ответ: $n=1,\ k=0$; $n=5, k=17$.

Признаки делимости на $2,4,5,10,25,\ 3,9,11$.

Определение. Десятичным представлением натурального числа называется представление числа в виде
$n=n_0+10n_1+100n_2+\ldots+10^k n_k$, где $0\leq n_i\leq 9, i=0,1,\ldots,k;\ n_k\neq 0$.
Сокращенная запись $n=\overline{n_k n_{k-1}\ldots n_1 n_0}$.

Утв.6 Пусть $n=\overline{n_k n_{k-1}...n_1 n_0}$ – десятичное представление числа числа n. Тогда:

1. Число n делится на 2 $\Leftrightarrow$ когда цифра n_0- четная;
2. Число n делится на 4 $\Leftrightarrow$ когда двузначное число $\overline{n_1 n_0}=n_0+10n_1$ делится на 4;
3. Число n делится на 5 $\Leftrightarrow$ когда $n_0=0$ либо $n_0=5$.
4. Число n делится на 10 $\Leftrightarrow$ когда $n_0=0$.
5. Число n делится на 25 $\Leftrightarrow$ когда двузначное число n_0+10n_1- делится на 25;
6. Число n делится на 3 $\Leftrightarrow$ когда сумма цифр числа n $N=n_0+n_1+n_2+...+n_k$ делится на 3;
7. Число n делится на 9 $\Leftrightarrow$ когда сумма цифр числа n $N=n_0+n_1+n_2+...+n_k$ делится на 9;
8. Число n делится на 11 $\Leftrightarrow$ когда сумма цифр числа n с чередующимися знаками $N=n_0-n_1+n_2-...+(-1)^k n_k$ делится на 11.

Доказательство. Доказательство признаков 1)-5) легко получается из десятичной записи числа $n=n_0+10n_1+100n_2+...+10^k n_k$. Докажем 6) и 7). Действительно,

$n=n_0+10n_1+100n_2+...+10^k n_k=n_0+n_1+9n_1+n_2+99n_2+...n_k+$

$+99...9n_k...$

Отсюда следует, что если n делится 3(или 9), то сумма цифр числа n тоже делится на 3(9).

Докажем 11). Пусть n делится на 11. Представим число n в виде

$n=n_0+10n_1+100n_2+...+10^k n_k=n_0+11n_1-n_1+n_2+99n_2+1001n_3$ $-n_3+....$ Так как все слагаемые суммы $11n_1+99n_2+1001n_3+...$ делятся на 11, то сумма $n_0-n_1+n_2-n_3+....$ тоже делится на 11. □

Определение. Число n сравнимо с числом m по модулю $p \Leftrightarrow n = p \cdot k + m$. Сокращенная запись – $n \equiv m (\mathrm{mod}\, p)$.

В терминах сравнений признаки делимости можно записать следующим образом:

1) $n \equiv n_0 \,(\mathrm{mod}2)$;
2) $n \equiv \overline{n_1 n_0} \,(\mathrm{mod}4)$;
3) $n \equiv n_0 \,(\mathrm{mod}5)$;
4) $n \equiv 0 (\mathrm{mod}10)$;
5) $n \equiv \overline{n_1 n_0} \,(\mathrm{mod}25)$;
6) $n \equiv (\, n_0 + n_1 + n_2 + ... + n_k) (\mathrm{mod}3)$;
7) $n \equiv (\, n_0 + n_1 + n_2 + ... + n_k) (\mathrm{mod}9)$;
8) $n \equiv (\, n_0 - n_1 + n_2 - n_3 + ...) (\mathrm{mod}11)$.

Признак делимости на 7 и 13.

Утв.7 Пусть $n = \overline{n_k n_{k-1} ... n_1 n_0}$ – десятичное представление числа числа n. Число n делится на $7 (13) \Leftrightarrow$ когда разность между числом n без трех последних знаков и числом, составленным из трех последних знаков, делится на $7 (13)$.

Доказательство. Представим n в виде $n = m \cdot 1000 + \overline{abc} = m \cdot (1001 - 1) + \overline{abc}$. Так как число 1001 делится на 7 и 13, то $m - \overline{abc}$ делится на 7 и 13. □

Пример 4. Пусть $n = 32109$. Тогда $32 - 109 = -77$ делится на 7 и, следовательно, число 32109 делится на 7. Пусть $n = 4925772124$. Тогда $4925772 - 124 = 4925648$; $4925 - 648 = 4277$; $4 - 277 = 273$ – делится на 13. Тогда число $n = 4925772124$ делится на 13.

Простые числа

Решето Эратосфена

(Простой алгоритм получения всех простые чисел)

Алгоритм. Выписываем все числа от 1 до 100 и вычеркиваем сначала все четные. Затем, из оставшихся вычеркиваем делящиеся на 3, 5, 7 и т.д. В результате останутся только простые числа.

Теорема Евклида. Число простых чисел бесконечно.

Доказательство "от противного". Пусть число простых чисел конечно - $p_1, p_2, ..., p_n$. Рассмотрим число $P = p_1 \cdot p_2 \cdot ....\cdot p_n + 1$, $P > p_k \; \forall k$. Вопрос: число P - простое или составное?

Если P - составное число, то оно делится на некоторое простое число p_k и, следовательно, единица делится на это простое число. Противоречие.

Если P- простое число, то оно больше любого простого числа p_k, а все простые числа мы выписали и пронумеровали. Опять противоречие. □

Утв.8 Если число n является составным, то оно имеет простой делитель p такой, что $p^2 \le n$.

Доказательство. Если p - наименьший простой делитель составного числа $n = m \cdot k$, то $p^2 \le m \cdot k = n$.

Следствие. Чтобы определить является ли число n простым, надо определить имеет ли оно простые делители $\le \sqrt{n}$.

Пример5. Пусть $n = 521$, $\sqrt{521} < 23$. Чтобы проверить, является ли число 521 простым, надо проверить, делится ли 521 на простые числа $3, 5, 7, 11, 13, 17, 19$. Ответ: число 521– простое.

Пример 6. Разложите на простые сомножители числа 1001 и 1591

Решение. Применим признаки делимости. Легко заметить, что 1001 делится на 11: $1001=11\cdot 91=11\cdot 7\cdot 13$. Число 1591 не подходит ни под один из признаков делимости, поэтому не делится на $2,3,5,7,11,13$. Для поисков дальнейшего разложения проверим все простые числа от 17 до $37\le\sqrt{1591}$. Делим число 1591 на простые числа $17,19,23,29,31,37$ получим, что $1591=37\cdot 43$.

Заманчивая сверхзадача теории чисел: найти формулу, позволяющую генерировать (получать) простые числа.

Утв. 9 Если $p=2^k+1$, то число 2^p+1 – составное.

Доказательство. $2^{2^k+1}+1=(2+1)(2^p-2^{p-1}+2^{p-2}-\ldots+1)$. Таким образом, если у числа p есть хотя бы один нечетный множитель, то число 2^p+1– составное. □

Генераторы простых чисел

Гипотеза: Все числа вида $F(n)=2^{2^n}+1$– простые.

При $n=1,2,3,4$ - это простые числа $5,17,257,65537$, для $n=5,6,\ldots 21$ вручную и с помощью компьютера доказано, что все числа составные.

Например, $F(5)=4294967297=641\cdot 6700417$ (Эйлер)

Гипотеза: Все числа вида $P(n)=\dfrac{10^n-7}{3}$– простые.

При $n=1,2,\ldots 8$– это так, а $P(9)=\dfrac{109-7}{3}$ делится на 17.

Гипотеза: Все числа вида $f(n)=n^2-n+41$– простые.

При $n=1,2,\ldots,40$ – это так, а $f(41)=41^2$.

Гипотеза: Все числа вида $f(n)=n^2-79n+1601-$ простые. При $n=1,2,...,79$ – это так, а $f(80)=41^2$.

Теорема. (Метод Ферма выделения множителей) Целое нечетное число p не является простым $\Leftrightarrow$ существуют натуральные числа n и k такие, что $p=n^2-k^2$. *Доказательство.* $\Leftarrow$ $p=n^2-k^2=(n-k)(n+k)$.

$\Rightarrow p=ab=\left(\frac{a+b}{2}\right)^2-\left(\frac{a-b}{2}\right)^2$. □

Пример 7. Разложить на простые сомножители числа $p=527, 1001, 493$.

$527+1=528, 527+4=531, 527+9=536, 527+16=543, 527+25=552,$

$527+36=563, 527+49=576=24^2 \Rightarrow 527=(24+7)(24-7)$.

Или $1001+32^2=2025=45^2 \Rightarrow 1001=13\cdot 77$.

Или $493+36=529=23^2 \Rightarrow 493=11\cdot 29$..

Пример 8. Разложить на множители число 2001. Это число делится на 3 $(2001=3\cdot 667)$. Далее, по методу выделения множителей, $667+9=676=26^2 \Rightarrow$

$667=(26+3)(26-3)=23\cdot 29$.

Пример 9. При каких целых n число $N=3n^4-8n^2-3$ – простое ?

Заметим, что $3n^4-8n^2-3=(n^2-3)(3n^2+1)=a\cdot b$. Так как $N-$простое, то либо $a=1$, либо $b=1$. Ответ: $n=\pm 2$.

Утв. 10 Натуральное число имеет нечетное число делителей $\Leftrightarrow$ когда оно является полным квадратом?

Доказательство. Если a – делитель числа n, то n имеет две различные пары делителей $\left(a;\frac{n}{a}\right)$ и $\left(\frac{n}{a};a\right)$, а при $a=\sqrt{n}$ обе пары будут равны.

Пример 10. Числа a, b имеют ровно по 99 делителей. Может ли число $a\cdot b$ иметь ровно 100 делителей?
Ответ: нет. Действительно по предыдущему свойству a и b - полные квадраты, а их произведение – нет.

Пример 11. Числа $p, 2p+1, 4p+1$ – простые. Найти p.
Ответ: $p=3$.

Пример 12. Числа $p, 8p^2+1$ – простые. Найти p. Ответ: $p=3$.

Для решения примеров 9-10 надо рассмотреть представление числа p через остатки от деления на 3.

НОД

Определение. Число d называется наибольшим общим делителем чисел a и b, если оно делит a и b, и является наибольшим из таких чисел.
Обозначение: $d = НОД(a,b)=(a,b)$.

Определение. Числа a и b называются взаимно простыми, если $(a,b)=1$.

Алгоритм Евклида
Пусть a, b – целые числа, $a>b$.
Разделим a на b с остатком, а затем на каждом шаге будем делить частное на остаток:

$a=bh_1+p_1,\ p_1<b;$

$b=p_1h_2+p_2,\ p_2<p_1;$

$p_1=p_2h_3+p_3, p_3<p_2;$

и т. д.

.
.

$p_{k-3} = p_{k-2}h_{k-1} + p_{k-1}$, $p_{k-1} < p_{k-2}$;

$p_{k-2} = p_{k-1}h_k + p_k$, $p_k < p_{k-1}$;

$p_{k-1} = p_k h_{k+1} + 0$.

Существует k такое, что $p_{k+1} = 0$, т.е. на каком-то шаге p_{k-1} разделится на p_k без остатка.

Утв. 11 Последний ненулевой остаток в алгоритме Евклида является наибольшим общим делителем чисел a и b, т.е. $p_k = (a, b)$.

*Доказательство. Пу*сть $d = (a, b)$ – наибольший общий делитель a, b. Докажем, что:

1) p_k является общим делителем a и b.

2) d делит p_k.

Отсюда будет следовать, что $d = p_k$. (Почему?)

1) Будем подниматься по алгоритму снизу вверх. Из последней строчки следует, что p_k делит p_{k-1}, из предпоследней, что - p_k делит p_{k-2},и т.д. Из алгоритма видно, что p_k делит все остатки. Тогда из первых двух строк следует, что p_k делит b и a.

2) Будем опускаться по алгоритму сверху вниз. Если $d = (a, b)$, то из первой строки следует, что d делит p_1. Из второй строки следует, что d делит p_2 и т.д. Получается, что d делит все остатки в алгоритме Евклида, а значит d делит p_k. □

Следствие1 . Существую числа u и v такие, что $d = a \cdot u + b \cdot v$

Действительно, из предпоследней строки можно выразить p_k через p_{k-1} и p_{k-2}, затем p_{k-1} выразить через p_{k-2} и p_{k-3}, и т.д. В результате, поднимаясь снизу вверх, можно получить требуемое выражение d через

p_1, p_2, а из первых двух строк – выражение d через a, b.

Алгоритм нахождения чисел u, v показан на примерах 11-14.

Следствие 2. Числа a и b взаимно простые $\Leftrightarrow$ существуют числа u и v такие, что $1 = a \cdot u + b \cdot v$.

Действительно, если $(a,b) = 1$, то из следствия 1 следует, что существую числа u и v такие, что $d = 1 = a \cdot u + b \cdot v$.

Обратно: если существую числа u и v такие, что $1 = a \cdot u + b \cdot v$, то $НОД(a,b)$ делит 1 и, следовательно, равен 1.

Следствие 3. $(a,b) = (a-b, b)$.

Например:

$(5a+3b, 13a+8b) = (5a+3b, 3a+2b) = (2a+b, 3a+2b) = (2a+b, a+b) =$

$(a, a+b) = (a,b)$;

$(2n+13, n+7) = (n+6, n+7) = (n+6, 1) = 1$;

$НОД(451, 287) = НОД(164, 287) = НОД(164, 123) = НОД(41, 123) = 41$;

$НОД(2^{100}-1, 2^{120}-1) = НОД(2^{100}-1, 2^{120}-2^{100}) =$

$НОД((2^{20}-1)(2^{80}+2^{60}+2^{40}+2^{20}+1), 2^{100}(2^{20}-1)) = (2^{20}-1) \cdot$

Пример13. Найти $НОД(85, 34)$ и выражение $НОД$ через a и b: $a = 85$, $b = 34$.

$85 = 34 \cdot 2 + 17$;	$a = b \cdot 2 + p_1$;
$34 = 17 \cdot 2 + 0$;	$b = p_1 \cdot 2 + 0$;
$d = 17$.	$d = p_1 = 17$.

$1 = p_1 = a - 2b$.

Пример14. Найти $НОД(203,91)$ и выражение $НОД$ через a и b: $a=203$, $b=91$.

$203=91\cdot 2+21;$	$a=b\cdot 2+p_1;$
$91=21\cdot 4+7;$	$b=p_1\cdot 4+p_2;$
$21=7\cdot 3+0,$	$p_1=p_2\cdot 3+0;$
$d=7.$	$d=p_2=7.$

$7=p_2=b-4p_1=b-4(a-2b)=9b-4a.$

Пример15. Найти $НОД(121,53)$ и выражение $НОД$ через a и b: $a=121$, $b=53$.

$121=53\cdot 2+15;$	$a=b\cdot 2+p_1;$
$53=15\cdot 3+8;$	$b=p_1\cdot 3+p_2;$
$15=8\cdot 1+7;$	$p_1=p_2\cdot 1+p_3;$
$8=7\cdot 1+1;$	$p_2=p_3\cdot 1+p_4;$
$7=7\cdot 1+0;$	$p_3=p_4\cdot 7+0,$
$d=1.$	$d=p_4=1.$

$1=p_4=p_2-p_3=p_2-(p_1-p_2)=2p_2-p_1=2(b-3p_1)-p_1=2b-7p_1=$
$=2b-7(a-2b)=16b-7a.$

Пример16. Найти $НОД(580,252)$ и выражение $НОД$ через a и b: $a=580$, $b=252$.

$580=252\cdot 2+76;$	$a=b\cdot 2+p_1;$
$252=76\cdot 3+24;$	$b=p_1\cdot 3+p_2;$
$76=24\cdot 3+4;$	$p_1=p_2\cdot 3+p_3;$
$24=4\cdot 6+0;$	$p_2=p_3\cdot 6+0;$
$d=4.$	$d=p_3=4.$

$1=p_3=p_1-3p_2=p_1-3(b-3p_1)=10p_1-3b=10(a-2b)-3b=10a-23b.$

Диофантовы уравнения

Определение. Уравнение вида $ax+by=c$ с целыми коэффициентами a, b относительно переменных x, y называются диофантовыми уравнениями.

Теорема Диофантовое уравнение $ax+by=c$ имеет решения в целых числах $\Leftrightarrow$ когда $НОД(a,b)$ делит c.

Доказательство. $\Rightarrow$ Если уравнение имеет целые решения, то $c=ax+by$ и, следовательно, $НОД$ чисел a, b делит c.

$\Leftarrow$ Укажем конструктивный алгоритм нахождения решений. Найдем $d=НОД(a,b)$. Разделим обе части уравнения на d и получим уравнение $a_1x+b_1y=c_1$, причем $НОД(a_1,b_1)=1$. Тогда существую числа u и v такие, что $1=a_1\cdot u+b_1\cdot v$. Домножим обе части уравнения на c_1 и получим $c_1=a_1\cdot(c_1u)+b_1\cdot(c_1v)=a_1\cdot x+b_1\cdot y$. Легко заметить, что $x_0=c_1u$, $y_0=c_1v$ являются решениями исходного уравнения □

Следствие. Если пара x_0, y_0 – решение исходного уравнения, то любая пара $x=x_0-b\cdot t$, $y=y_0+a\cdot t$ при $t\in Z$ является решением исходного уравнения.

Доказательство осуществляется непосредственной подстановкой значений x и y в уравнение $ax+by=c$.

Пример 17. Решить уравнение $19x-15y=2$

Решение. $(19,15)=1$ $\Rightarrow$ Из алгоритма Евклида находим числа u и v такие, что $1=19\cdot u+15\cdot v, u=4, v=-5$, т.е. $1=19\cdot 4-15\cdot 5$. Умножим обе части равенства на $c=2$ и получим равенство $2=19\cdot 8-15\cdot 10$, т.е. $x_0=8$, $y_0=10$. Общее решение будет иметь вид $x=8-15\cdot t$, $y=10+19\cdot t$.

Пример 18. Доказать, что следующие уравнения не имеют решений: $39x-3y=13$; $2x-4y=21$.

Действительно, коэффициенты этих уравнений не удовлетворяют условию теоремы.

Пример 19. Решить уравнение $203x+91y=14$

Решение. $(203,91)=7 \Rightarrow$ Разделим обе части уравнения на 7 и получим новое уравнение $29x+13y=2$, причем $(29,13)=1$. Из алгоритма Евклида находим числа u и v такие, что $1=29\cdot u+13\cdot v, u=-4, v=9$, т.е. $1=29\cdot(-4)+13\cdot 9$. Умножим обе части равенства на $c_1=2$ и получим равенство $2=29\cdot(-8)+13\cdot 18$, т.е. $x_0=-8,\ y_0=18$. Общее решение будет иметь вид $x=8-91\cdot t$, $y=18+203\cdot t$.

Пример 20. Решить в натуральных числах уравнение $y+x^{2006}=HOK(x,y)$.

Решение. Пусть $HOK(x,y)=d \Rightarrow {}^{d}\!/_{x} \Rightarrow {}^{y}\!/_{x} \Rightarrow HOK(x,y)=y.$ Следовательно, уравнение имеет вид $y+x^{2006}=y \Rightarrow x=0 \Rightarrow y=0$. Ответ: Решений нет.

Основная теорема арифметики

Теорема. Любое натуральное число больше 1 либо является простым числом, либо может быть записано в виде произведения простых чисел, причем это произведение единственно с точностью до порядка сомножителей.

Доказательство теоремы разбивается на несколько лемм.

Лемма 1. Всякое натуральное число либо равно 1, либо простое, либо - произведение простых.

Доказательство по индукции. Для $n=1,2,3,4,...$ лемма верна. Предположим, что лемма верна для любого $n<k$ и докажем, что она верна для $n=k$

Возможны два варианта:

1) $k-$простое $\Rightarrow$ и лемма верна,

2) $k-$составное $\Rightarrow k=a\cdot b$, причем $a,b<k \Rightarrow$ из предположения индукции, что a и b либо простые, либо произведения простых. □

Лемма 2. Если простое p число делит произведение ab, то p делит a либо p делит b.

Доказательство. Пусть p не делит a. Тогда существуют числа u и v такие, что $1 = a \cdot u + p \cdot v$. Домножим обе части равенства на b и получим $b = ba \cdot u + bp \cdot v$. Отсюда следует, что b делится на p. □

Лемма 3. Если простое число p делит произведение чисел $q_1 q_2 ... q_n$, то p делит одно из чисел q_k $(k = 1, 2, ..., n)$.

Доказательство индукцией по числу сомножителей. При $n = 1, 2$ лемма верна. Пусть p делит произведение k сомножителей $q_1 q_2 ... q_k$. Докажем, что p делит произведение $q_1 q_2 ... q_k \cdot q_{k+1}$. Пусть $a = q_1 q_2 ... q_k$, $b = q_{k+1}$. Тогда p делит произведение ab, и, следовательно, делит a либо - b. Если p делит q_{k+1}, то все доказано, а если p делит $q_1 q_2 ... q_k$, то по предположению p делит одно из чисел $q_m, m = 1, 2, ..., k$. □

Лемма 4. Если простое число p делит произведение простых чисел $q_1 q_2 ... q_n$, то p равно одному из чисел q_k $(k = 1, 2, ..., n)$.

Доказательство. По лемме 3, если p делит произведение чисел $q_1 q_2 ... q_n$, то p делит одно из чисел $q_1, q_2, ..., q_n$. Но если p делит одно из простых чисел q_k, то $p = q_k$. □

Доказательство теоремы следует из лемм 1-4. *Докажем единственность* индукцией по числу сомножителей. Пусть $q_1 q_2 ... q_n = p_1 p_2 .... p_m$ – два разложения одного числа. Если $n = 1$ или $n = 2$, то единственность следует из лемм 3-4. Предположим, что единственность выполняется для $k = n - 1$. Если p_1 делит произведение $q_1 q_2 .... q_n$, то p_1 одно из чисел $q_k, k = 1, 2, ..., m$. Сократим обе части равенства на p_1 и получим равенство, в котором $k = n - 1$. □

Следствие 1. Пусть $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, $b = q_1^{m_1} q_2^{m_2} \dots q_m^{m_s}$. Тогда $НОД(a,b)$ равен произведению всех общих простых сомножителей с наименьшими степенями.

Следствие 2. Пусть $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, $b = q_1^{k_1} q_2^{k_2} \dots q_m^{m_s}$. Тогда $НОК(a,b)$ равно произведению всех различных простых сомножителей с наибольшими степенями.

Следствие 3. $ab = НОК(a,b) \cdot НОД(a,b)$.

Пример 21. Пусть $a = 2^3 \cdot 3 \cdot 5^4 \cdot 13$, $b = 2 \cdot 5^3 \cdot 13^3 \cdot 19$.

Тогда $НОД(a,b) = 2 \cdot 5 \cdot 13$, $НОК(a,b) = 2^3 \cdot 3 \cdot 5^4 \cdot 13^3 \cdot 19$.

Утв.12 Если произведение двух взаимно простых сомножителей является квадратом, то каждый сомножитель является квадратом.

Доказательство. Пусть $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, $b = q_1^{k_1} q_2^{k_2} \dots q_m^{m_n}$. Так как a и b взаимно простые, то в их разложении участвуют различные простые сомножители. Тогда в произведении $c^2 = ab = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n} \cdot q_1^{k_1} q_2^{k_2} \dots q_m^{m_n}$, которое является квадратом, все простые сомножители различные и имеют четные показатели. □

Утв.13 Пусть $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$.

Тогда сумма всех делителей числа a равна

$$\sigma(a) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \dots \cdot \frac{p_n^{k_n+1} - 1}{p_n - 1}.$$

Действительно, общий делитель числа a имеет вид $a = p_1^{t_1} p_2^{t_2} \dots p_n^{t_n}$ $(0 \le t_i \le k_i, i = 1 \dots n)$, а сумма делителей равна

$$\sigma(a) = (1 + p_1 + p_1^2 + \dots + p_1^{k_1})(1 + p_2 + p_2^2 + \dots + p_2^{k_2}) \dots (1 + p_n + p_n^2 + \dots + p_n^{k_n}).$$

Далее по формуле суммы членов геометрической прогрессии получаем исходное выражение. □

Например, $\sigma(360) = \sigma(2^3 \cdot 3^2 \cdot 5) = \frac{2^4 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 1170$.

Утв.14 Пусть $a = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$. Тогда число различных делителей числа a равно $N(a) = (1+k_1)(1+k_2)\ldots(1+k_n)$.

Действительно, число $N(a)$ равно числу сомножителей в формуле $\sigma(a)$. □

Пример 22. (Демо 2010)

1) Найти все числа, которые делятся на 42 и имеют ровно 42 различных делителя.

2) Найти все числа, которые делятся на 10 и имеют ровно 15 различных делителей.

Решение.

1) Так как $42 = 2 \cdot 3 \cdot 7$, то исходное число a делится на $2, 3, 7$ и по Утв.13 $N(a) = (1+k_1)(1+k_2)(1+k_3) = 42 = 2 \cdot 3 \cdot 7$.

Следовательно, a может иметь только три различных простых сомножителя 2, 3 и 7, степени которых могут быть равны 1, 2 или 5.

Ответ: $42 \cdot 3 \cdot 2^5, 42 \cdot 7 \cdot 2^5, 42 \cdot 2 \cdot 3^5, 42 \cdot 7 \cdot 3^5, 42 \cdot 2 \cdot 7^5, 42 \cdot 3 \cdot 7^5$.

2) Так как $10 = 2 \cdot 5$, то исходное число a делится на $2(5)$ и по Утв.13 $N(a) = (1+k_1)(1+k_2)(1+k_3) = 15 = 3 \cdot 5$.

Следовательно, a может иметь только два различных простых сомножителя 2 и 5, степени которых равны 2 или 4. Ответ: 2500, 400.

Пример 23.(Окружная олимпиада 2006) Найти все натуральные числа n, удовлетворяющие условию $n! = \overline{123\ldots n}$.

Решение 1. Если $n > 5$, то число $\overline{123\ldots n}$ имеет столько нулей, сколько их у числа n, а число $n!$ имеет по крайней мере на один нуль больше $(2 \cdot 5 = 10)$. Следовательно, $n \le 5$.

Выпишем все возможные значения факториалов: $1! = 1,\ 2! = 2 \ne 12,\ 3! = 6 \ne 123,\ 4! = 24 \ne 1234, 5! = 120 \ne 12345$.

Решение 2. Докажем, что $\forall n > 1\ \ \overline{123\ldots n} > n!$.

Действительно, если b $k-$значное число, то $\overline{ab}=a\cdot 10^k+b>a\cdot 10^k>a\cdot b$. Ответ: $n=1$.

Пример 24. Найти все пары натуральных чисел, наименьшее общее кратное которых равно 78, а наибольший общий делитель равен 13.

Решение. Пусть $a,b-$исходные числа. Так как $13-$простое число, а $78=13\cdot 3\cdot 2$, то по следствиям основной теоремы арифметики только число 13 входит в разложение обоих чисел, а для чисел 2 и 3 возможны варианты: $(a,b)=(13,13\cdot 2\cdot 3)=(13\cdot 2,13\cdot 3)=(13\cdot 3,13\cdot 2)$.
Ответ: $(a,b)=(13,78)=(26,39)=(39,26)$.

Пример 25. Решите в целых числах уравнение $2xy=x^2+2y$

Решение. Из уравнения следует, что x делится на 2, т.е. $x=2n$. Подставим это значение x в уравнение, получим $2\cdot 2\cdot n\cdot y=4n^2+2y$ и сократим на 2: $2\cdot n\cdot y=2n^2+y$. Откуда следует, что y делится на 2, т.е. $y=2p$. Тогда уравнение имеет вид $2\cdot n2p=2n^2+4p\Rightarrow 2np=n^2+p\Rightarrow p(2n-1)=n^2$. Так как $2n-1$ не делится на n, то p делится на n^2, т.е. $p=t\cdot n^2$ и $t\cdot(2n-1)=1$. Отсюда $t=1,\ 2n-1=1\Rightarrow x=2,y=2$.
Ответ: $x=2,y=2$.

Пример 26. Решите в целых числах уравнение $x!+y!=10z+9$.

Решение. Из уравнения следует, что справа стоит нечетное число, следовательно, $x=1$ либо $y=1$. В противном случае оба числа $x!$ и $y!$ будут четными. Пусть $x=1$. Тогда $1+y!=10z+9\ \Rightarrow y!=10z+8$. Отсюда следует, что $y<5$, иначе 8 будет делится на 5. Следовательно, $y=1,2,3,4$. Рассмотрим все эти случаи: $y=1\Rightarrow 1=10z+8\Rightarrow\varnothing$; $y=2\Rightarrow 2=10z+8\Rightarrow\varnothing$; $y=3\Rightarrow 6=10z+8\Rightarrow\varnothing$; $y=4\Rightarrow 24=10z+8\Rightarrow\varnothing$.
Ответ: решений нет.

Решето Эратосфена

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
19 20 21 22 23 24 25 26 27 28 29 30 31 32
33 34 35 36 37 38 39 40 41 42 43 44 45 46
47 48 49 50 51 52 53 54 55 56 57 58 59 60
61 62 63 64 65 66 67 68 69 70 71 72 73 74
75 76 77 78 79 80 81 82 83 84 85 86 87 88
89 90 91 92 93 94 95 96 97 98 99 100

101 102 103 104 105 106 107 108 109 110
111 112 113 114 115 116 117 118 119 120
121 122 123 124 125 126 127 128 129 130
131 132 133 134 135 136 137 138 139 140
141 142 143 144 145 146 147 148 149 150
151 152 153 154 155 156 157 158 159 160
161 162 163 164 165 166 167 168 169 170
171 172 173 174 175 176 177 178 179 180
181 182 183 184 185 186 187 188 189 190
191 192 193 194 195 196 197 198 199 200

201 202 203 204 205 206 207 208 209 210 211
212 213 214 215 216 217 218 219 220 221 222
223 224 225 226 227 228 229 230 231 232 233
234 235 236 237 238 239 240 241 242 243 244
245 246 247 248 249 250 251 252 253 254 255
256 257 258 259 260 261 262 263 264 265 266
267 268 269 270 271 272 273 274 275 276 277
278 279 280 281 282 283 284 285 286 287 288
289 290 291 292 293 294 295 296 297 298 299
300