ДЕЛИМОСТЬ ЧИСЕЛ И ПРИЛОЖЕНИЯ

Ф.Г.Шлейфер

Первый вариант этой статьи был написан 40 лет назад и посвящалась она доказательству одного важного частного случая знаменитой теоремы Дирихле о бесконечности множества простых чисел в арифметических прогрессиях. В доказательстве использовались многие свойства делимости целых чисел. Некоторые из этих свойств я считал известными, а другие доказывал. Уже не помню, почему одни свойства отделил от других. Знание всех этих свойств и умение доказывать их я считаю важным для математического образования старшеклассников и студентов-математиков пединститутов. Этот материал будет полезен также учителям математики, т.к. слишком часто многие факты (делимости целых чисел) даются в школе без доказательств. Поэтому первая часть статьи представляет учебный материал по теории делимости целых чисел. Если Вы считаете, что хорошо владеете этим материалом, то переходите сразу к приложениям.

Часть 1. Делимость целых чисел.

§ 1. Деление целых чисел.

Определение. Говорят, что целое число A делится на целое число B ($A \vdots B$), если существует ещё одно целое число C такое, что $A=B\cdot C$. При этом C называют частным от деления A на B.

Несколько простых выводов.

1) Любое число делится на 1: $A=1\cdot A$.
2) Любое число делится на себя: $A=A\cdot 1$.
3) Никакое число, кроме 0, не делится на 0, т.к. $A=0\cdot C$ имеет место только для $A=0$. Но всё-таки делится 0 на 0 или нет? Согласно определению 0 делится на 0, но на роль частного при этом подходит любое число.

Теорема 1.1.1. Для целых чисел A,B,C справедливы следующие утверждения.

1) Если A делится на B и B делится на C, то A делится на C .
2) Если A и B делятся на C, то $A\pm B$ делится на C.
3) Для каждого натурального n разность A^n-B^n делится на $A-B$.
4) Для каждого натурального нечётного n сумма A^n+B^n делится на $A+B$.

Доказательство. 1) Существуют целые числа M и K такие, что $A=B\cdot M$ и $B=C\cdot K$. Но тогда $A= C\cdot K\cdot M$ и A делится на C.

2) Существуют целые числа M и K такие, что $A=C\cdot M$ и $B=C\cdot K$. Но тогда $A\pm B=C(M\pm K)$ и $A\pm B$ делится на C.

3) При $2\le n$ справедливо равенство $A^n-B^n=(A-B)\cdot(A^{n-1}+A^{n-2}B+A^{n-3}B^2+\ldots+B^{n-1})$, откуда и следует требуемая делимость. При $n=1$ утверждение очевидно.

4) При нечётных $n\ge 3$ справедливо равенство $A^n+B^n=(A+B)\cdot(A^{n-1}-A^{n-2}B+A^{n-3}B^2-\ldots+B^{n-1})$, откуда и следует требуемая делимость. При $n=1$ утверждение очевидно.

Теорема 1.1.2. Пусть $\{A_1,A_2,\ldots,A_n\}$ и $\{B_1,B_2,\ldots,B_n\}$ - два набора целых чисел, причём все соответствующие разности A_1-B_1, A_2-B_2, …, A_n-B_n делятся на число C. Тогда

1) $(A_1+A_2+\ldots+A_n)-(B_1+B_2+\ldots+B_n)$ делится на C,

2) $(A_1\cdot A_2\cdot\ldots\cdot A_n)-(B_1\cdot B_2\cdot\ldots\cdot B_n)$ делится на C.

Доказательство. По условию существуют целые числа $Q_1, Q_2, Q_3, \ldots, Q_n$ такие, что $A_1-B_1=CQ_1$, $A_2-B_2=CQ_2,\ldots$, $A_n-B_n=CQ_n$.

1) $(A_1+A_2+\ldots+A_n)-(B_1+B_2+\ldots+B_n)=C\cdot(Q_1+Q_2+\ldots+Q_n)$ очевидно делится на C.

2) Построим (n+1) новых чисел так: $M_i=B_1\cdot B_2\cdot\ldots\cdot B_i\cdot A_{i+1}\cdot\ldots\cdot A_n$, где i=0,1,2,…,n. Уточним, $M_0=A_1\cdot A_2\cdot\ldots\cdot A_n$ и $M_n=B_1\cdot B_2\cdot\ldots\cdot B_n$. Далее заметим, что разность соседних новых чисел делится на C: $M_i-M_{i+1}=B_1\cdot B_2\cdot\ldots\cdot B_i\cdot A_{i+1}\cdot\ldots\cdot A_n-B_1\cdot B_2\cdot\ldots\cdot B_{i+1}\cdot A_{i+2}\cdot\ldots\cdot A_n=$ $=B_1\cdot B_2\cdot\ldots\cdot B_i\cdot(A_{i+1}-B_{i+1})\cdot A_{i+2}\cdot\ldots\cdot A_n=B_1\cdot B_2\cdot\ldots\cdot B_i\cdot C\cdot Q_{i+1}\cdot A_{i+2}\cdot\ldots\cdot A_n$. Следовательно, $(A_1\cdot A_2\cdot\ldots\cdot A_n)-(B_1\cdot B_2\cdot\ldots\cdot B_n)=M_0-M_n=(M_0-M_1)+(M_1-M_2)+\ldots+(M_{n-1}-M_n)$ делится на C.

§ 2. Деление с остатком.

Определение. Разделить целое число A на целое число B с остатком означает записать A в следующем виде: $A=Bq+r$, где q и r некоторые целые числа и $0\le r<|B|$ (через $|B|$ обозначена абсолютная величина числа B).

Из определения не видно, существует ли для данных чисел A и B требуемая пара чисел q и r? И, если существует, то обязательно ли одна? Сразу можно отметить, что никакое число невозможно разделить с остатком на 0, т.к. не существует числа r такого, что $0\le r<0$.

Теорема 1.2.1. Для целых чисел A и B ($B\neq0$) существуют целые числа q и r такие, что $A=Bq+r$ и $0\le r<|B|$. Более того такая пара чисел q и r – единственная.

Доказательство. 1) Пусть $0\le A$ и $0<B$. Если $A<B$, то требуемая запись получается без всяких усилий: $A=B\cdot0+A$, т.к. $0\le A<B$. Пусть теперь $B\le A$. Рассмотрим убывающую последовательность целых чисел: A, A–B, A–2B, A–3B,…. . Очевидно, что начиная с некоторого места в данной последовательности будут находится отрицательные числа. Рассмотрим последнее неотрицательное число в последовательности: $0\le r=A-Bq$, т.е. следующее число в последовательности A–B(q+1) – уже отрицательное, т.е. $A-B(q+1)<0$ или $r=A-Bq<B$. Таким образом, найдена требуемая пара чисел: q и r.

2) Пусть теперь $A<0$ и $0<B$. Рассмотрим возрастающую последовательность чисел: A, A+B, A+2B, A+3B,…. . Очевидно, что начиная с некоторого места в данной последовательности будут находится неотрицательные числа. Рассмотрим первое из них: $0\le r=A+Bq$ и отметим, что предыдущее число A+B(q–1) – уже отрицательное, т.е. $r=A+Bq<B$. Таким образом найдена требуемая пара чисел: –q и r.

3) Пусть, наконец, $B<0$. Для чисел A и –B существует требуемая пара целых чисел q и r (пункты 1-2): $A=(-B)q+r$, причём $0\le r<-B$. Но тогда пара чисел -q и r как раз удовлетворяет равенству $A=B(-q)+r$, причём $0\le r<-B=|B|$.

4) Переходим к доказательству единственности пары q и r. Пусть найдены 2 пары, именно, $A=Bq+r$ и $A=Bq_1+r_1$, причём $0\le r<|B|$ и $0\le r_1<|B|$. Примем для определённости $r\le r_1$ и запишем очевидное равенство $B(q-q_1)=r_1-r$. В правой части равенства стоит число из промежутка $[0;|B|-1]$, но лишь одно число из этого промежутка (а именно – 0) делится на $|B|$. Таким образом, $r=r_1$ и $q=q_1$.

Замечание. Полезно отметить множество {0, 1, 2,…., n–1} всех остатков от деления целых чисел на натуральное число n. Причём остаток равный 0 соответствует случаю, когда целое число делится на n.

Теорема 1.2.2. Пусть A, B - целые числа, n – натуральное число. (A–B) ⋮ n тогда и только тогда, когда A и B дают равные остатки при делении на n.

Доказательство. Разделим A и B на n с остатком: $A=nq+r$, $B=nq_1+r_1$. Если $r=r_1$, то $A–B= n(q–q_1)$ ⋮ n. Если $r\neq r_1$, то $A–B= n(q–q_1)+(r–r_1)$ не делится на n, т.к. число $r–r_1\neq 0$ и находится в промежутке [–(n–1); n–1], а в этом промежутке только 0 делится на n.

Теорема 1.2.3. Пусть $A=nq+r$ – деление с остатком целого числа A на натуральное число n. Пусть, далее, X пробегает (увеличиваясь) n последовательных целых значений, начиная с A. При r=0 остатки от деления X на n будут последовательно возрастать от 0 до n–1. При $1\leq r$ остатки от деления X на n сначала будут последовательно возрастать от r до n–1, затем упадут до 0, и затем снова будут возрастать до r–1.

Доказательство. Если r=0, то n равенств: A=nq+0, A+1=nq+1,….,A+(n–1)=nq+(n–1) являются как раз записями деления с остатком n последовательных чисел на n. Чуть сложнее в других случаях, когда $1\leq r$. Рассмотрим сначала n–r последовательных чисел: A=nq+r, A+1=nq+r+1,…., A+(n–r–1)=nq+r+(n–r–1)=nq+(n–1) и затем оставшиеся r чисел: A+(n–r) = nq+r+(n–r) = n(q+1)+0, A+(n–r+1) = nq+r+(n–r+1) = n(q+1)+1,……., A+(n–1) = =nq+r+(n–1) = n(q+1)+(r–1).

Следствие. Произведение n последовательных целых чисел делится на n. Сумма n последовательных целых чисел делится на n только, если n – нечётное число.

Доказательство. Ввиду теорем 1.2.2 и 1.1.2 вместо последовательных чисел можно рассматривать их остатки от деления на n. Ввиду теоремы 1.2.3 этими остатками являются 0, 1, 2, …, n–1. Произведение остатков равно 0 и, следовательно, произведение n последовательных целых чисел делится на n. Сумма остатков равна n(n–1)/2, что тоже делится на n, если n – нечётное число и не делится на n, если n – чётное число.

§ 3. Наибольший общий делитель нескольких чисел. Взаимно простые числа.

Определение. Пусть $(a_1, a_2,…., a_n)$ – конечная последовательность целых чисел. Наибольшим общим делителем этих чисел называют натуральное число d, удовлетворяющее двум условиям: 1) d – общий делитель данных чисел, т.е. a_1 ⋮ d, a_2 ⋮ d,…., a_n ⋮ d;

2) Для любого общего делителя b данных чисел имеет место d ⋮ b.

Теорема 1.3.1. Пусть $(a_1, a_2,…., a_n)$ – конечная последовательность целых чисел, хотя бы одно из которых отлично от нуля. Существует наибольший общий делитель d данных чисел, причём только один. Кроме того, d можно записать в виде суммы $d=x_1a_1+x_2a_2+….+ +x_na_n$, где $x_1, x_2,…., x_n$ – некоторые целые числа.

Доказательство. Рассмотрим множество M всех чисел вида $x_1a_1+ x_2a_2+….+ x_na_n$, где $x_1, x_2,…., x_n$ – произвольные целые числа.

1) Покажем, что в M есть натуральные числа. Число $a_1=1\cdot a_1+0\cdot a_2+\ldots+0\cdot a_n$ содержится в M и аналогично числа $a_2,\ldots, a_n$ содержатся в M. Следовательно, в M найдутся числа a_i и $-a_i$ отличные от 0. Одно из них будет натуральным числом.

2) Обозначим через d наименьшее натуральное число в M. Согласно определению M справедливо равенство $d=p_1a_1+p_2a_2+\ldots+p_na_n$ для некоторых целых чисел $p_1, p_2,\ldots, p_n$. Легко видеть, что все числа кратные d содержатся в M. Покажем, что других чисел в M нет. Действительно, пусть b – произвольное число из M, т.е. $b=s_1a_1+s_2a_2+\ldots+s_na_n$ для некоторых целых чисел $s_1, s_2,\ldots, s_n$. Разделим b с остатком на d: $b=dq+r$, где $0\le r<d$. Остаётся заметить, что $r=b-dq=(s_1-qp_1)a_1+(s_2-qp_2)a_2+\ldots+(s_n-qp_n)a_n$ содержится в M. Но по условию в M нет натуральных чисел меньших d, следовательно, r=0 и $b\vdots d$.

3) В пункте 1 показано, что числа $a_1, a_2,\ldots, a_n$ содержатся в M. В пункте 2 показано, что каждое число из M делится на d. Следовательно, все числа $a_1, a_2,\ldots, a_n$ делятся на d. Пусть теперь c – общий делитель чисел $a_1, a_2,\ldots, a_n$. Тогда и $d=p_1a_1+p_2a_2+\ldots+p_na_n$ тоже делится на c. Таким образом, d – наибольший общий делитель чисел $a_1, a_2,\ldots, a_n$. Кроме того, возможность записать равенство $d=p_1a_1+p_2a_2+\ldots+p_na_n$ уже установлена в пункте 2. Наконец, равенство двух натуральных чисел, каждое из которых делится на другое, проверяется непосредственно.

Замечание. Конечная последовательность нулей не обладает наибольшим общим делителем просто потому, что 0 делится на любое натуральное число. Во всех остальных случаях будем писать $НОД(a_1,a_2,\ldots,a_n)$ для обозначения наибольшего общего делителя чисел $a_1,a_2,\ldots,a_n$.

Практический приём. Как вычислить $НОД(a_1, a_2,\ldots, a_n)$? Предлагаю следующую последовательность действий.

1) Заменим в данном наборе чисел все отрицательные числа на противоположные. Выбросим из данного набора чисел нули и повторяющиеся числа.

2) Выбираем наименьшее из данных чисел и обозначим его через r.

3) Начинаем делить данные числа, кроме r, с остатком на r. Если остаток равен 0, то выкидываем соответствующее число из последовательности данных чисел и переходим к делению следующего из данных чисел на r. Аналогично будем поступать пока остатки от деления равны 0. Если среди данных чисел осталось лишь одно число – r, то процесс закончен: $НОД(a_1, a_2,\ldots, a_n)=r$. Пусть теперь найдётся остаток отличный от 0 и, разумеется, он меньше r. Заменим делимое на этот остаток и далее именно этот остаток будет играть роль r. Возвращаемся к пункту 3.

Так как натуральное число r постоянно уменьшается, то процесс не может продолжаться бесконечно. Остаётся проверить, что r удовлетворяет определению наибольшего общего делителя данных чисел.

Пример. Вычислим НОД(84, 252, 1001, 364).

$252=84\cdot3+0$ => выкидываем число 252: (84, 252, 1001, 364) => (84, 1001, 364),
$1001=84\cdot11+77$ => заменяем число: (84, 1001, 364) => (84, 77, 364),
$84=77\cdot1+7$ => заменяем число: (84, 77, 364) => (7, 77, 364),
$77=7\cdot11+0$ => выкидываем число 77: (7, 77, 364) => (7, 364),
$364=7\cdot52+0$ => выкидываем число 364: (7, 364) => (7).

Всё, нашли НОД(84, 252, 1001, 364)=7.

Практический приём (Алгоритм Евклида). Для двух натуральных чисел a и b приведённый выше практический приём становится ещё прозрачнее, записываем цепочку делений с остатком, пока не получим в первый раз нулевой остаток:

$a=bq_1+r_1$,

$b=r_1q_2+r_2$,

$r_1=r_2q_3+r_3$,

……..

$r_{n-1}=r_nq_{n+1}+r_{n+1}$,

$r_n=r_{n+1}q_{n+2}+0$. НОД(a, b) $=r_{n+1}$.

Определение. Целые числа $a_1, a_2,\ldots, a_n$ называют взаимно простыми, если НОД($a_1, a_2,\ldots, a_n$)=1.

Теорема 1.3.2. Пусть $a_1, a_2,\ldots, a_n$, b – целые числа, причём НОД(a_1,b) = НОД(a_2,b) = =…=НОД(a_n,b) =1. Тогда НОД($a_1\cdot a_2\cdot\ldots\cdot a_n$, b)=1.

Доказательство. 1) Рассмотрим сначала случай n=2. Как доказано в теореме 1.3.1, существуют целые числа u_1,u_2,v_1,v_2 такие, что $u_1a_1+v_1b=1$ и $u_2a_2+v_2b=1$. Перемножим эти равенства: $u_1u_2a_1a_2+(u_1a_1v_2+v_1u_2a_2+v_1bv_2)\cdot b=1$. Откуда видно, что 1 делится на любой общий делитель чисел $a_1\cdot a_2$ и b, следовательно, НОД($a_1\cdot a_2$, b)=1.

2) Согласно пункту 1 из НОД($a_1\cdot a_2$, b) = НОД(a_3, b) = 1 следует НОД($a_1\cdot a_2\cdot a_3$, b) =1. Аналогично из НОД($a_1\cdot a_2\cdot a_3$, b) = НОД(a_4, b) = 1 следует НОД($a_1\cdot a_2\cdot a_3\cdot a_4$, b) =1. И т.д. до конца.

Теорема 1.3.3. Пусть ab делится на c, причём a и c – взаимно простые числа. Тогда b делится на c.

Доказательство. Согласно теореме 1.3.1, существуют целые числа u,v такие, что ua+vc =1. Умножим это равенство на b: uab+vcb = b. Оба слагаемых в левой части равенства делятся на c. Следовательно, b делится на c.

Теорема 1.3.4. Пусть a, n, m, d – натуральные числа, причём 1<a и d = НОД(n,m). Тогда НОД(a^n-1, a^m-1) = a^d-1. (Аналогичный факт приведён, как задача 6 в моей статье «Об одном методе решения задач на делимость чисел»).

Доказательство. По условию n и m делятся на d. Следовательно, существуют натуральные числа u и v, что справедливы равенства: n=du и m=dv. Ввиду теоремы 1.1.1 (пункт 3) $a^n-1=(a^d)^u-1$ и $a^m-1=(a^d)^v-1$ делятся на a^d-1.

Пусть теперь a^n-1 и a^m-1 делятся на целое число b. Остаётся доказать, что a^d-1 делится на b. Во–первых, ввиду очевидного равенства $a^n-(a^n-1)=1$ можно сделать вывод, что a и b – взаимно простые числа. Во–вторых, существуют целые числа p и q такие, что np+mq=d (теорема 1.3.1). Очевидно, что одно из чисел p и q – положительное, а другое отрицательное. Достаточно рассмотреть один случай: p – положительное и q – отрицательное, и далее полагаем s=–q. Легко установить следующие факты делимости целых чисел: $(a^{nq}-1)\vdots(a^n-1)\vdots b$, $(a^{ms}-1)\vdots(a^m-1)\vdots b$, $a^{ms}\cdot(a^{nq-ms}-1)=(a^{nq}-1)-(a^{ms}-1)\vdots b$,

$a^{d}-1=a^{nq-ms}-1 \vdots b$. Лишь последнюю делимость поясним: она следует из предыдущей делимости на основании теорем 1.3.2 и 1.3.3.

§ 4. Простые числа. Основная теорема арифметики. Малая теорема Ферма.

Определение. Натуральное число называют простым, если у него имеется ровно два натуральных делителя (1 и само число). Если у натурального числа имеется более двух натуральных делителей, то его называют составным (это число можно разложить в произведение нескольких сомножителей).

Примеры. Числа 3, 29, 73 являются простыми. Числа 1, 4, 100 не являются простыми.

Теорема 1.4.1. Множество простых чисел бесконечно (это было известно ещё в Древней Греции).

Доказательство. Пусть уже известны n простых чисел: $p_1, p_2, p_3,\ldots, p_n$. Нашей целью является указать ещё одно (n+1) – ое простое число. Рассмотрим число $S=p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n+1$. Если S – простое число, то оно и будет новым (n+1) – ым простым числом. Пусть теперь S – составное число. Разложим S в произведение простых множителей (очевидно, это возможно) и обозначим через q – один из этих простых множителей. Если допустить, что $q=p_1$, то получим, что $1=S-p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$ делится на p_1, что невозможно. Также приводят к противоречию допущения $q=p_2$, $q=p_3$,…., $q=p_n$. Следовательно, q – новое (n+1) – ое простое число.

Практический приём (Решето Эратосфена). Пусть требуется выделить все простые числа в промежутке от 1 до n. Следующий алгоритм позволяет это сделать. Выпишем подряд все числа от 2 до n. Вычислим число q так, чтобы $n<q^2$ (для уменьшения вычислений желательно выбрать q как можно меньше).

Находим первое неподчёркнутое и незачёркнутое число в наших записях (сначала вообще нет подчёркнутых или зачёркнутых чисел), пусть им будет a. Если $q \le a$, то процесс закончен, причём все незачёркнутые числа и дают полный список простых чисел от 1 до n. В противном случае подчёркиваем число a и после него начинаем «считалку»: 1,2,3,….,a – на счёт «a» вычёркиваем число и начинаем снова считать с 1. Так продолжаем, пока не дойдём до n. Важно отметить, что в «считалке» участвуют все числа: как зачёркнутые, так и незачёркнутые. Возвращаемся к началу абзаца.

Пример решета Эратосфена. Пусть требуется выделить простые числа из промежутка от 1 до 35. В качестве числа q возьмём q=6. Выпишем все числа подряд, начиная с 2:
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.
В первой «считалке» a=2:
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~~.
Во второй «считалке» a=3:
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~~.
В третьей «считалке» a=5:
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~~.
Четвёртой «считалки» для a=7 уже не будет, т.к. q=6<7. Получился набор всех простых чисел от 1 до 35: 2,3,5,7,11,13,17,19,23,29,31.

Теорема 1.4.2. В результате применения решета Эратосфена действительно будут выделены все простые числа из рассмотренного промежутка.

Доказательство. Сохраним обозначения, сделанные в решете Эратосфена. Сначала отметим, что при каждой «считалке» на счёт “a” вычёркиваются только составные числа:

2a, 3a, … . Пусть теперь k – произвольное составное число, причём $k \le n$. Обозначим через p – наименьший простой делитель k. Можно записать равенство k=ps и, далее, $p^2 \le ps = k \le n < q^2$, т.е. p<q и, следовательно, число k будет вычеркнуто в «считалке» при a=p.

Теорема 1.4.3 (Основная теорема арифметики). Для каждого натурального числа, большего 1, существует единственное разложение в произведение простых множителей (с точностью до перестановки сомножителей).

Доказательство. 1) Если p – простое число и n – произвольное натуральное число, то НОД(n, p) = 1 или НОД(n, p) = p, т.к. p делится только на 1 и на p. Следовательно, либо n делится на p, либо n и p – взаимно простые числа. И далее, произведение простых чисел, отличных от данного простого числа p, не делится на p (теорема 1.3.2).

2) Пусть теперь натуральное число n имеет два разложения на простые множители: $n=p^i \cdot a = p^j \cdot b$, причём среди простых делителей a и b уже не встречается простое число p. Тогда a и b не делятся на p (пункт 1). Если допустить, что i<j, то после сокращения на p^i получим, что a делится на p – противоречие. Аналогичное противоречие получим, если j<i. Таким образом, непременно выполняется i=j, т.е. в двух разложениях n на простые множители простое число p входит равное число раз. И это верно для любого простого делителя n.

А сейчас докажем лемму, которую используем при доказательстве следующих теорем.

Лемма. Пусть p – простое число и a – натуральное число, которое не делится на p. Тогда остатки от деления на p чисел a, 2a, 3a, …., (p–1)a можно так перенумеровать, что получится последовательность (1, 2, 3, …., p–1).

Доказательство. Разделим на p с остатком следующие числа: $a=pq_1+r_1$, $2a=pq_2+r_2$, $3a=pq_3+r_3$, …., $(p-1)a=pq_{p-1}+r_{p-1}$. Покажем, что все полученные остатки (а их всего p–1) разные и отличны от 0. Действительно, a не делится на p, следовательно, НОД(a, p)=1. Аналогично НОД(1, p)=1, НОД(2, p)=1, НОД(3, p)=1, …., НОД(p–1, p)=1. Следовательно (теорема 1.3.2), НОД(a, p)=1, НОД(2a, p)=1, …., НОД((p–1)a, p)=1. Таким образом, среди остатков $r_1, r_2, r_3, \ldots, r_{p-1}$ нет равного 0. Далее (теорема 1.2.2), два числа дают одинаковые остатки при делении на p тогда и только тогда, когда разность этих чисел делится на p, но разности данных чисел снова содержатся среди данных чисел, а выше уже установлено, что все данные числа взаимно просты с p.

Теорема 1.4.4 (Малая теорема Ферма). Пусть p – простое число и a – натуральное число, которое не делится на p. Тогда $a^{p-1}-1$ делится на p.

Доказательство. Разделим на p с остатком следующие (p–1) чисел: $a=pq_1+r_1$, $2a=pq_2+r_2$, $3a=pq_3+r_3$, …., $(p-1)a=pq_{p-1}+r_{p-1}$. В лемме установлено, что последовательность $(r_1, r_2, r_3, \ldots, r_{p-1})$ отличается от последовательности (1,2,3,…, p–1) только порядком членов, следовательно, $r_1 \cdot r_2 \cdot r_3 \cdot \ldots \cdot r_{p-1} = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$. Теперь, ввиду теоремы 1.1.2(п.2), можно утверждать, что разность $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a - 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a - r_1 \cdot r_2 \cdot r_3 \cdot \ldots \cdot r_{p-1}$ делится на p. Вынесем общий множитель за скобку $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a - 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \cdot (a^{p-1}-1)$ делится на p. А т.к. все множители 1, 2, 3,…,(p–1) взаимно просты с p, то $a^{p-1}-1$ делится на p (теорема 1.3.3).

Теорема 1.4.5 (Вильсон). Пусть p – простое число, тогда $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)+1$ делится на p.

Доказательство. Будем полагать, что 5≤p (для p=2 и p=3 утверждение легко проверить). Два числа a и b из последовательности (2,3,…, p–2) назовём братьями, если ab–1 делится на p. Ввиду леммы у каждого числа a есть брат b, причём только один. Почему из рассмотрения выброшены числа 1 и p–1? Очень просто – это исключительные случаи, когда в качестве брата выступает само первоначальное число: x^2–1 делится на p тогда и только тогда, когда x–1 делится на p или x+1 делится на p, т.е. x=1 или x=p–1. Ещё заметим, что первоначальное число является братом для своего брата. Таким образом, все числа из последовательности (2, 3, …, p–2) распадаются на пары братьев. Теперь будем вычислять произведение $2\cdot3\cdot\ldots\cdot(p-2)=B_1\cdot B_2\cdot\ldots\cdot B_s$, где s=(p–3)/2 – количество братских пар, а $B_1,B_2,\ldots,B_s$ – произведения чисел в соответствующих братских парах. Ввиду теоремы 1.1.2, разность $B_1\cdot B_2\cdot\ldots\cdot B_s$–1 делится на p. Окончательно, $1\cdot2\cdot3\cdot\ldots\cdot(p-1)+1=B_1\cdot B_2\cdot\ldots\cdot B_s\cdot(p-1)+1=(B_1\cdot B_2\cdot\ldots\cdot B_s-1)\cdot(p-1)+p$ делится на p.

Часть 2. Простые числа в арифметических прогрессиях.

В середине XIX века знаменитый немецкий математик Дирихле доказал теорему о бесконечности множества простых чисел в бесконечной арифметической прогрессии, первый член и разность которой – натуральные взаимно простые числа. Наша цель много более скромная: доказать бесконечность множества простых чисел в бесконечной арифметической прогрессии, разность которой – натуральное число, а первый член равен 1.

§ 1. Определения и предварительные факты.

Определение. Натуральный делитель b натурального числа a называем главным делителем a, если НОД(a/b, b)=1. (Это определение встречается в моей статье «Об одном методе решения задач на делимость чисел»).

Определение. Пусть a – произвольное натуральное число. Последовательность $(b_1, b_2,\ldots, b_k)$ некоторых натуральных делителей числа a будем называть полной, если произведение этих делителей, взятых достаточное число раз, делится на a.

Пример. (2, 5) – полная последовательность делителей числа 40.

Теорема 2.1.1. Если $(b_1, b_2,\ldots, b_k)$ – полная последовательность делителей числа a, и все эти делители являются главными, то уже $b_1\cdot b_2\cdot\ldots\cdot b_k$ делится на a.

Доказательство. Пусть p – произвольный простой делитель a. Пусть, далее, p^n – наибольшая степень p, на которую делится a. Найдётся в полной последовательности делителей $(b_1, b_2,\ldots, b_k)$ хотя бы одно число b_i, которое делится на p. Если допустить, что b_i не делится на p^n, то получим, что a/b_i делится на p и НОД$(a/b_i, b_i)\neq1$, что противоречит условию: b_i – главный делитель a. Таким образом, b_i делится на p^n. Ввиду произвольности простого делителя p, можно утверждать, что $b_1\cdot b_2\cdot\ldots\cdot b_k$ делится на a.

Теорема 2.1.2. Главные делители b и c натурального числа a образуют полную последовательность делителей тогда и только тогда, когда b·c=a·НОД(b, c).

Доказательство. Пусть p – произвольный простой делитель a, причём p^n – наибольшая степень p, на которую делится a. Возможны четыре случая.

1) Ни одно из чисел b и c не делятся на p. Тогда последовательность (b, c) не является полной и равенство b·c=a·НОД(b, c) не выполняется.

2) b делится, но c не делится на p. Тогда b делится на p^n (ведь b – главный делитель!) и, далее, p^n – наивысшая степень p, на которую делятся и b·c, и a·НОД(b, c).

3) c делится, но b не делится на p. Этот случай рассматривается также, как предыдущий.

4) b и c одновременно делятся на p. Тогда b и c делятся на p^n (ведь b и c – главные делители!) и, далее, p^{2n} – наивысшая степень p, на которую делятся и b·c, и a·НОД(b, c).

Таким образом, если для всех простых делителей числа a будут иметь место случаи 2-4, то, во-первых, b·c делится на a и, во-вторых, для чисел b·c и a·НОД(b, c) получаются одинаковые представления в виде произведений простых чисел, т.е. b·c=a·НОД(b, c).

Теорема 2.1.3. Пусть простое число p является делителем натуральных чисел n и a. Пусть, далее, n = p·k. Тогда a^k-1 является главным делителем числа a^n-1.

Доказательство. Обозначим $x=a^k$ и тогда, согласно определению, остаётся только доказать, что НОД(x–1, $x^{p-1}+x^{p-2}+\ldots+x+1$)=1. Действительно, $(x^{p-1}-1)+(x^{p-2}-1)+\ldots+(x-1)$ делится на x–1 (Теорема 1.1.1, пункт 3) и, следовательно, для некоторого целого числа T можно записать $(x^{p-1}-1)+(x^{p-2}-1)+\ldots+(x-1)=(x-1)\cdot T$ и, далее, $p = (x^{p-1}+x^{p-2}+\ldots+x+1)-(x-1)\cdot T$. Таким образом, простое число p делится на НОД(x–1, $x^{p-1}+x^{p-2}+\ldots+x+1$). Но x–1 не делится на p, т.к. $x=a^k$ делится на p. Следовательно, НОД(x–1, $x^{p-1}+x^{p-2}+\ldots+x+1$)=1.

Обозначение. Пусть $(a_1, a_2, \ldots, a_n)$ – конечная последовательность чисел, причём на этот раз не обязательно целых, но рациональных, и k – натуральное число из промежутка [1; n]. Строим всевозможные последовательности длины k, образованные членами первоначальной последовательности с возрастающими номерами: $A_1, A_2,\ldots,A_t$. В комбинаторике доказывают, что $t = n\cdot(n-1)\cdot(n-2)\cdot\ldots\cdot(n-k+1)/(1\cdot2\cdot\ldots\cdot k)$. Для каждой из построенных последовательностей вычислим произведение её членов. Наконец, через S_k или, более подробно, через $S_k(a_1,a_2,\ldots,a_n)$ обозначим сумму всех указанных произведений. Это обозначение будет использоваться в данном и следующем параграфах.

Примеры. $S_1(a_1,a_2,\ldots,a_n)= a_1+a_2+\ldots+a_n$ – сумма содержит n слагаемых.

$S_2(a_1,a_2,\ldots,a_n)= (a_1\cdot a_2+ a_1\cdot a_3+\ldots+ a_1\cdot a_n) +(a_2\cdot a_3+ a_2\cdot a_4+\ldots+ a_2\cdot a_n) +\ldots+ (a_{n-1}\cdot a_n)$ – сумма содержит n(n–1)/2 слагаемых.

$S_3(a_1,a_2,\ldots,a_n)=(a_1\cdot a_2\cdot a_3+a_1\cdot a_2\cdot a_4+\ldots+a_1\cdot a_2\cdot a_n)+(a_1\cdot a_3\cdot a_4+a_1\cdot a_3\cdot a_5+\ldots+a_1\cdot a_3\cdot a_n)+\ldots+(a_{n-2}\cdot a_{n-1}\cdot a_n)$ – сумма содержит n(n–1)(n–2)/6 слагаемых.

$S_n(a_1,a_2,\ldots,a_n)= a_1\cdot a_2\cdot a_3\cdot\ldots\cdot a_n$ – только одно слагаемое.

Теорема 2.1.4. Пусть $(a_1, a_2, \ldots, a_n)$ – конечная последовательность рациональных чисел. Имеет место равенство $(1- a_1)\cdot(1- a_2)\cdot\ldots\cdot(1- a_n) = 1 - S_1+ S_2- S_3+\ldots+ (-1)^n\cdot S_n$.

Доказательство достаточно простое, несмотря на громоздкий результат. Итак, нам нужно перемножить n двучленов, в каждом из которых есть 1 и есть выражение вида $-a_i$. Нетрудно видеть, что всего получится 2^n произведений, которые нужно будет сложить. Если в конкретном произведении будет чётное число выражений вида $-a_i$, то знак перед

ним будет "+", в противном случае знак будет "–". Подсчитаем отдельно суммы таких произведений, в которые вошло одинаковое количество (скажем k) сомножителей вида $-a_i$. Легко видеть, что в такую сумму войдут всевозможные произведения, содержащие k сомножителей вида $-a_i$. Но такая сумма и обозначалась выше через S_k (со знаками мы разобрались раньше).

Обозначение. Пусть $(a_1, a_2, \ldots, a_n)$ – конечная последовательность натуральных чисел, и k – натуральное число из промежутка [1; n].

1) Строим всевозможные последовательности длины k, образованные членами первоначальной последовательности с возрастающими номерами: $A_1, A_2, \ldots, A_t$. Выше уже отмечалось, что $t = n\cdot(n-1)\cdot(n-2)\cdot\ldots\cdot(n-k+1)/(1\cdot2\cdot\ldots\cdot k)$.

2) Для каждой последовательности вычисляем наибольший общий делитель её членов: $НОД(A_1), НОД(A_2), \ldots, НОД(A_t)$.

3) Перемножим все полученные выше наибольшие общие делители и произведение их обозначим через $ПНОД_k(a_1, a_2, \ldots, a_n)$ или просто $ПНОД_k$, когда понятно о каких числах идёт речь. Это обозначение будет использоваться в данном и следующем параграфах.

Теорема 2.1.5. Пусть $(a_1, a_2, \ldots, a_n)$ – полная последовательность делителей числа m, и все эти делители являются главными. Тогда справедливо равенство
$m = ПНОД_1\cdot(1/ ПНОД_2)\cdot ПНОД_3\cdot(1/ ПНОД_4)\cdot\ldots$ (всего n сомножителей).

Доказательство. Пусть p^i – главный делитель m, где p – простое число и $0<i$. Пусть, далее, $a_1, a_2, \ldots, a_s$ делятся на p , а остальные числа $a_{s+1}, a_{s+2}, \ldots, a_n$ не делятся на p. Заметим, что p^i – главный делитель чисел $a_1, a_2, \ldots, a_s$, т.к. эти числа в свою очередь – главные делители m. Таким образом, p^{is} – главный делитель числа $ПНОД_1 = a_1\cdot a_2\cdot\ldots\cdot a_n$. Чуть сложнее для $ПНОД_2$. Среди чисел $НОД(a_u, a_v)$ имеется ровно $s(s-1)/2$ делящихся на p (это имеет место, если $1\le u<v\le s$), причём в этих случаях p^i будет главным делителем $НОД(a_u, a_v)$. Следовательно, $p^{is(s-1)/2}$ – главный делитель числа $ПНОД_2$. Переходим к общему случаю $ПНОД_k$. Если $s<k$, то легко понять, что среди k чисел из первоначальной последовательности хотя бы одно число не делится на p и, следовательно, их наибольший общий делитель не делится на p, а тогда и $ПНОД_k$ не делится на p. А что будет, если $k\le s$? Существует ровно $t = s\cdot(s-1)\cdot(s-2)\cdot\ldots\cdot(s-k+1)/(1\cdot2\cdot\ldots\cdot k)$ последовательностей длины k, составленных из чисел $a_1, a_2, \ldots, a_s$, причём наибольший общий делитель для каждой из этих последовательностей имеет p^i своим главным делителем. Таким образом, p^{it} – главный делитель числа $ПНОД_k$.

Из комбинаторики известно равенство для биномиальных коэффициентов: $1 = s - s(s-1)/2 + s(s-1)(s-2)/3\cdot2 - s(s-1)(s-2)(s-3)/4\cdot3\cdot2 + \ldots$ Следовательно, в доказываемом равенстве простой делитель p входит в одинаковой степени i как в левую так и правую часть. Наконец, нетрудно заметить, что выражение справа не может делиться на простые числа, на которые не делится m.

§ 2. Основной результат.

Теорема 2.2.1. В бесконечной арифметической прогрессии с первым членом 1 и разностью, являющейся натуральным числом, содержится бесконечное множество простых чисел.

Доказательство. Обозначим через d – разность данной прогрессии (полагаем 1<d). Пусть далее, $p_1, p_2, \ldots, p_n$ – все простые делители d, a , $q_1, q_2, \ldots, q_m$ – простые числа уже найденные в данной прогрессии. Наша цель: найти в данной прогрессии новое простое число q_{m+1} (сравните с доказательством теоремы 1.4.1). Рассмотрим число $a=p_1 \cdot p_2 \cdot \ldots \cdot p_n \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_m \cdot v$, где v – некоторое натуральное число, которое уточним позже.

Числа $b_1 = a^{d/p_1}-1$, $b_2 = a^{d/p_2}-1$, …., $b_n = a^{d/p_n}-1$ являются главными делителями числа a^d-1 по теореме 2.1.3. Первой нашей целью является доказать, что последовательность $(b_1, b_2, \ldots, b_n)$ делителей числа a^d-1 не является полной. Для этого докажем неравенство $\text{ПНОД}_1(b_1, b_2, \ldots, b_n)\cdot(1/\text{ПНОД}_2(b_1, b_2, \ldots, b_n))\cdot\text{ПНОД}_3(b_1, b_2, \ldots, b_n)\cdot\ldots < a^d-1$ (в левой части n сомножителей), которое вместе с теоремой 2.1.5 установит требуемый факт. Рассмотрим раздельно сомножители в левой части и найдём для них соответствующие неравенства. $\text{ПНОД}_1(b_1, b_2, \ldots, b_n) = b_1 \cdot b_2 \cdot \ldots \cdot b_n < (a^{d/p_1})\cdot(a^{d/p_2})\cdot\ldots\cdot(a^{d/p_n}) = a^{dS_1}$, где $S_1 = S_1(1/p_1, 1/p_2, \ldots, 1/p_n)$.

Переходим к сомножителю $\text{ПНОД}_2(b_1, b_2, \ldots, b_n)$, который находится в знаменателе и, следовательно, для него нужно получить неравенство обратного вида. $\text{ПНОД}_2(b_1, b_2, \ldots, b_n) = \text{НОД}(b_1, b_2)\cdot\text{НОД}(b_1, b_3)\cdot\ldots\cdot\text{НОД}(b_{n-1}, b_n) = (a^{d/p_1p_2}-1)\cdot(a^{d/p_1p_3}-1)\cdot\ldots\cdot(a^{d/p_{n-1}p_n}-1)$, ввиду теоремы 1.3.4. Далее, воспользуемся неравенством x/2<x–1 (для 1<x): $a^{dS_2}/2^{t_2} = (a^{d/p_1p_2})\cdot(a^{d/p_1p_3})\cdot\ldots\cdot(a^{d/p_{n-1}p_n})/2^{t_2} < (a^{d/p_1p_2}-1)\cdot(a^{d/p_1p_3}-1)\cdot\ldots\cdot(a^{d/p_{n-1}p_n}-1)$, где $S_2 = S_2(1/p_1, 1/p_2, \ldots, 1/p_n)$ и $t_2 = n(n-1)/2$ – количество слагаемых в S_2.

Переходим к сомножителю $\text{ПНОД}_3(b_1, b_2, \ldots, b_n)$. $\text{ПНОД}_3(b_1, b_2, \ldots, b_n) = \text{НОД}(b_1, b_2, b_3)\cdot\text{НОД}(b_1, b_2, b_4)\cdot\ldots\cdot\text{НОД}(b_{n-2}, b_{n-1}, b_n) = (a^{d/p_1p_2p_3}-1)\cdot(a^{d/p_1p_2p_4}-1)\cdot\ldots\cdot(a^{d/p_{n-2}p_{n-1}p_n}-1)$, ввиду теоремы 1.3.4. Увеличим каждый сомножитель на 1 и получим: $\text{ПНОД}_3(b_1, b_2, \ldots, b_n) < a^{dS_3}$, где $S_3 = S_3(1/p_1, 1/p_2, \ldots, 1/p_n)$.

Рассмотрим ещё сомножитель $\text{ПНОД}_4(b_1, b_2, \ldots, b_n)$, который находится в знаменателе и, следовательно, для него нужно получить неравенство обратного вида. $\text{ПНОД}_4(b_1, b_2, \ldots, b_n) = \text{НОД}(b_1, b_2, b_3, b_4)\cdot\ldots\cdot\text{НОД}(b_{n-3}, b_{n-2}, b_{n-1}, b_n) = (a^{d/p_1p_2\,p_3p_4}-1)\cdot\ldots\cdot(a^{d/p_{n-3}p_{n-2}p_{n-1}p_n}-1)$, ввиду теоремы 1.3.4. Далее воспользуемся неравенством x/2<x–1 (для 1<x): $a^{dS_4}/2^{t_4} = (a^{d/p_1p_2p_3p_4})\cdot\ldots\cdot(a^{d/p_{n-3}p_{n-2}p_{n-1}p_n})/2^{t_4} < (a^{d/p_1p_2p_3p_4}-1)\cdot\ldots\cdot(a^{d/p_{n-3}p_{n-2}p_{n-1}p_n}-1)$, где $S_4 = S_4(1/p_1, 1/p_2, \ldots, 1/p_n)$ и $t_4 = n(n-1)(n-2)(n-3)/(4\cdot3\cdot2)$ – количество слагаемых в S_4.

Далее аналогично продолжаем до конца. И тогда получим неравенство $\text{ПНОД}_1(b_1, b_2, \ldots, b_n)\cdot(1/\text{ПНОД}_2(b_1, b_2, \ldots, b_n))\cdot\text{ПНОД}_3(b_1, b_2, \ldots, b_n)\cdot\ldots < (a^{dS_1-dS_2+dS_3-dS_4+\ldots})\cdot 2^{t_2+t_4+\ldots} = a^{d(1-(1-1/p_1)(1-1/p_2)\ldots(1-1/p_n))}\cdot 2^{t_2+t_4+\ldots}$ (теорема 2.1.4) $\le a^{d-1}\cdot 2^{t_2+t_4+\ldots}$ (т.к. $1 \le d\cdot(1-1/p_1)\cdot(1-1/p_2)\cdot\ldots\cdot(1-1/p_n)$) $= a^{d-1}\cdot v$ (вот и пришло время определить число $v = 2^{t_2+t_4+\ldots}$) $\le a^d-1$. Итак, доказано, что последовательность $(b_1,\ldots,b_n)$ делителей числа a^d-1 не является полной. Но это как раз и означает, что существует

простой делитель q числа a^d-1, который не является делителем чисел $b_1, b_2,\ldots, b_n$. Очевидно, что q не совпадает ни с одним из простых чисел $q_1, q_2, \ldots, q_m$, т.к. эти числа являются делителями числа a. И осталось лишь доказать, что простое число q содержится в данной арифметической прогрессии. По теореме Ферма (1.4.4) $a^{q-1}-1$ также делится на q. Следовательно, и НОД(a^d-1, $a^{q-1}-1$) делится на q, и, далее, $a^{НОД(d,\ q-1)}-1$ делится на q. Если допустить, что (q–1) не делится на d, то НОД(d, q–1) окажется делителем d, отличным от d, а это означает, что одно из чисел d/p_1, d/p_2, …., d/p_n будет делиться на НОД(d, q-1) и, далее, соответсвующее число из последовательности $(b_1, b_2,\ldots, b_n)$ делиться на $a^{НОД(d,\ q-1)}-1$, и, следовательно, делится на q, но выше омечено, что это не так. Таким образом, (q–1) делится на d, т.е. q содержится в данной арифметической прогрессии.

Часть 3. Арифметика гауссовых чисел.

В этой главе будем рассматривать целые гауссовы числа , т.е. числа вида **a**+**bi**, где **a** и **b** – целые числа, а **i** – мнимая единица, т.е. $\mathbf{i}^2=-1$. Предполагается, что Вы знакомы с комплексными числами, хотя даже, если это не так, то Вы можете принять на веру «существование» мнимой единицы, а далее всё будет понятно. Отметим, что все целые числа являются также и гауссовыми (**a**+0·**i**). Далее, для гауссовых чисел полностью сохраняется содержание § 1 части 1.

§ 1. Гауссовы числа. Основные свойства. Деление с остатком.

Определение. Гауссовы числа **a**+**bi** и **a**–**bi** называют сопряжёнными. Если A – гауссово число, то сопряжённое к нему число обозначим A^*. Нормой гауссова числа **a**+**bi** будем называть целое неотрицательное число $\|\mathbf{a}+\mathbf{bi}\| = \mathbf{a}^2+\mathbf{b}^2$. Заметим, что также можно определить норму и для любого комплексного числа **a**+**bi**, с действительными **a** и **b** (нам это потребуется в доказательстве теоремы 3.1.5).

Теорема 3.1.1. Норма произведения (двух) гауссовых чисел равна произведению норм сомножителей.

Доказательство. $\|(\mathbf{a}+\mathbf{bi})\cdot(\mathbf{c}+\mathbf{di})\|=\|(\mathbf{ac}-\mathbf{bd})+(\mathbf{ad}+\mathbf{bc})\mathbf{i}\|=(\mathbf{ac}-\mathbf{bd})^2+(\mathbf{ad}+\mathbf{bc})^2\|= (\mathbf{a}^2\mathbf{c}^2+\mathbf{b}^2\mathbf{d}^2+ +\mathbf{a}^2\mathbf{d}^2+\mathbf{b}^2\mathbf{c}^2=(\mathbf{a}^2+\mathbf{b}^2)(\mathbf{c}^2+\mathbf{d}^2) =\|(\mathbf{a}+\mathbf{bi})\|\cdot\|(\mathbf{c}+\mathbf{di})\|$. Для большего числа сомножителей нужно применить индукцию.

Теорема 3.1.2. Для гауссовых чисел справедливо равенство: $(A_1\cdot A_2\cdot\ldots\cdot A_n)^* = A_1^*\cdot A_2^*\cdot\ldots\cdot A_n^*$.

Доказательство. Пусть A_1=**a**+**bi** и A_2=**c**+**di**, тогда $(A_1A_2)^*$= ((**ac**–**bd**)+(**ad**+**bc**)**i**)* = (**ac**–**bd**) – (**ad**+**bc**)**i** = (**a**–**bi**)(**c**–**di**) = $A_1^*\cdot A_2^*$. Для большего числа сомножителей нужно применить индукцию.

Теорема 3.1.3. Пусть (**a**+**bi**)(**c**+**di**) = **n** – натуральное число, причём **a**≠0, **b**≠0, **c**≠0, **d**≠0 и НОД(**a, b**)=НОД(**c**, **d**)=1. Тогда (**a**+**bi**) и (**c**+**di**) – сопряжённые числа и $\mathbf{n} = \mathbf{a}^2+\mathbf{b}^2$.

Доказательство. Из равенства (**a**+**bi**)(**c**+**di**) = **n** вытекает **ad**+**bc** = 0. Далее, во-первых, из **ad** ⋮ **b** и НОД(**a, b**)=1 следует (теорема 1.3.3), что **d** ⋮ **b**. Во-вторых, из **bc** ⋮ **d** и

НОД($\mathbf{c}$, $\mathbf{d}$) =1 следует (теорема 1.3.3), что $\mathbf{b} \vdots \mathbf{d}$. Таким образом, имеет место $\mathbf{d} = \pm\mathbf{b}$. В случае $\mathbf{d} = \mathbf{b}$ приходим к $\mathbf{c} = -\mathbf{a}$ и $\mathbf{n} = (\mathbf{a}+\mathbf{bi})(-\mathbf{a}+\mathbf{bi}) = -(\mathbf{a}^2+\mathbf{b}^2)<0$, что противоречит условию. Следовательно, имеет место $\mathbf{d} = -\mathbf{b}$ и далее $\mathbf{c} = \mathbf{a}$ и $\mathbf{n} = (\mathbf{a}+\mathbf{bi})(\mathbf{a}-\mathbf{bi}) = \mathbf{a}^2+\mathbf{b}^2$.

Определение. Два гауссовых числа назовём родственниками, если одно из них получается из другого умножением на одно из четырёх чисел: 1, –1, **i**, –**i**. Отметим, что эти четыре числа – как раз те, у которых норма равна 1.

Теорема 3.1.4. Если каждое из двух гауссовых чисел, отличных от 0, делится на другое, то они – родственники. Справедливо также обратное утверждение.

Доказательство. Нормы двух данных чисел равны, что вытекает из теоремы 3.1.1. Следовательно норма частного от деления равна 1, т.е. данные числа – родственники.

Теорема 3.1.5 (Деление с остатком). Пусть A и B – гауссовы числа, причём B≠0. Существуют гауссовы числа Q и R такие, что $A=B\cdot Q+R$ и $\|R\|<\|B\|$.

Доказательство. Пусть A = $\mathbf{a}+\mathbf{bi}$ и B = $\mathbf{c}+\mathbf{di}$. Запишем цепочку равенств $\mathbf{a}+\mathbf{bi} = (\mathbf{a}+\mathbf{bi})\cdot(\mathbf{c}+\mathbf{di})(\mathbf{c}-\mathbf{di})/(\mathbf{c}^2+\mathbf{d}^2) = (\mathbf{c}+\mathbf{di})((\mathbf{ac}+\mathbf{bd})+(\mathbf{bc}-\mathbf{ad})\mathbf{i})/(\mathbf{c}^2+\mathbf{d}^2)$. Вычислим целые числа **u** и **v**, как самые близкие к рациональным числам $(\mathbf{ac}+\mathbf{bd})/(\mathbf{c}^2+\mathbf{d}^2)$ и $(\mathbf{bc}-\mathbf{ad})/(\mathbf{c}^2+\mathbf{d}^2)$ соответственно. Таким образом, можно записать $(\mathbf{ac}+\mathbf{bd})/(\mathbf{c}^2+\mathbf{d}^2) = \mathbf{u}+\boldsymbol{\delta}$ и $(\mathbf{bc}-\mathbf{ad})/(\mathbf{c}^2+\mathbf{d}^2) = \mathbf{v}+\boldsymbol{\varepsilon}$, где $\boldsymbol{\delta}$ и $\boldsymbol{\varepsilon}$ – подходящие рациональные числа из промежутка [– ½; ½]. Добавим к цепочке равенств ещё два $\mathbf{a}+\mathbf{bi} = (\mathbf{c}+\mathbf{di})((\mathbf{u}+\boldsymbol{\delta})+(\mathbf{v}+\boldsymbol{\varepsilon})\mathbf{i}) = (\mathbf{c}+\mathbf{di})(\mathbf{u}+\mathbf{vi})+(\mathbf{c}+\mathbf{di})(\boldsymbol{\delta}+\boldsymbol{\varepsilon}\mathbf{i})$. Теперь полагаем $Q=\mathbf{u}+\mathbf{vi}$ и $R=(\mathbf{c}+\mathbf{di})(\boldsymbol{\delta}+\boldsymbol{\varepsilon}\mathbf{i})$, причём $\|R\| = \|(\mathbf{c}+\mathbf{di})(\boldsymbol{\delta}+\boldsymbol{\varepsilon}\mathbf{i})\| = \|(\mathbf{c}+\mathbf{di})\|\cdot\|(\boldsymbol{\delta}+\boldsymbol{\varepsilon}\mathbf{i})\| = \|(\mathbf{c}+\mathbf{di})\|\cdot(\boldsymbol{\delta}^2+\boldsymbol{\varepsilon}^2) \le \|(\mathbf{c}+\mathbf{di})\|\cdot ½$.

Замечание. Обязательно ли было выбирать целые числа **u** и **v** самыми близкими к соответствующим дробям? Нет необязательно, но условие $\boldsymbol{\delta}^2+\boldsymbol{\varepsilon}^2 <1$ непременно должно выполняться. Следовательно, **u** и **v** должны быть соседними к указанным дробям, т.е. в любом случае будет не более 4-х остатков, но иногда может быть и меньше. Например, при делении $\mathbf{5}+\mathbf{i}$ на $\mathbf{1}+\mathbf{3i}$ могут получиться только 3 разных остатка: $\mathbf{5}+\mathbf{i} = (\mathbf{1}+\mathbf{3i})\cdot(-\mathbf{i})+(\mathbf{2}+\mathbf{2i})$, $\mathbf{5}+\mathbf{i} = (\mathbf{1}+\mathbf{3i})\cdot(\mathbf{1}-\mathbf{i})+(\mathbf{1}-\mathbf{i})$ и $\mathbf{5}+\mathbf{i} = (\mathbf{1}+\mathbf{3i})\cdot(\mathbf{1}-\mathbf{2i})+(-\mathbf{2})$. Таким образом, деление с остатком для гауссовых целых чисел возможно, но частное и остаток определяются неоднозначно.

§ 2. Наибольший общий делитель нескольких гауссовых чисел. Взаимно простые гауссовы числа.

Совершенно аналогично целым числам определим и докажем существование наибольшего общего делителя для последовательности гауссовых чисел.

Определение. Пусть $(A_1, A_2, \ldots, A_n)$ – конечная последовательность гауссовых чисел. Наибольшим общим делителем этих чисел называют гауссово число D, удовлетворяющее двум условиям: 1) D – общий делитель данных чисел, т.е. $A_1 \vdots D$, $A_2 \vdots D, \ldots, A_n \vdots D$.

2) Для любого общего делителя B данных чисел имеет место $D \vdots B$.

Теорема 3.2.1. Пусть $(A_1, A_2, \ldots, A_n)$ – конечная последовательность гауссовых чисел, хотя бы одно из которых отлично от нуля. Существуют наибольшие общие делители данных чисел, причём все они – родственники. Кроме того, их можно записать в виде суммы $P_1A_1+P_2A_2+\ldots+P_nA_n$, где $P_1, P_2, \ldots, P_n$ – некоторые гауссовы числа.

Доказательство. Рассмотрим множество M всех чисел вида $X_1A_1+X_2A_2+\ldots+X_nA_n$, где $X_1, X_2, \ldots, X_n$ – произвольные гауссовы числа.

1) Очевидно, что M содержит гауссовы числа $A_1, A_2, \ldots, A_n$, так например, $A_1 = 1\cdot A_1 +$

$+0\cdot A_2+\ldots+0\cdot A_n$. Следовательно, в M есть числа отличные от нуля.

2) Обозначим через D гауссово число из M с наименьшей положительной нормой (если таких чисел несколько, то рассмотрим любое из них). Согласно определению M справедливо равенство $D=P_1A_1+P_2A_2+\ldots+P_nA_n$ для некоторых гауссовых чисел $P_1,P_2,\ldots,P_n$. Легко видеть, что все числа кратные D содержатся в M. Покажем, что других чисел в M нет. Действительно, пусть B – произвольное число из M, т.е. $B=S_1A_1+S_2A_2+\ldots+S_nA_n$ для некоторых гауссовых чисел $S_1, S_2,\ldots, S_n$. Разделим B с остатком на D: $B=DQ+R$, где $\|R\|<\|D\|$. Остаётся заметить, что $R = B-DQ = (S_1-QP_1)A_1+(S_2-QP_2)A+\ldots+(S_n-QP_n)A_n$ содержится в M. Но по условию в M нет гауссовых чисел отличных от 0 с нормой меньшей, чем $\|D\|$. Следовательно, R=0 и B⋮D.

3) В пункте 1 отмечено, что числа $A_1, A_2,\ldots, A_n$ содержатся в M. В пункте 2 показано, что каждое число из M делится на D. Следовательно, все числа $A_1, A_2,\ldots, A_n$ делятся на D. Пусть теперь C – общий делитель чисел $A_1, A_2,\ldots, A_n$. Тогда и $D=P_1A_1+P_2A_2+\ldots+P_nA_n$ тоже делится на C. Таким образом, D – наибольший общий делитель чисел $A_1, A_2,\ldots, A_n$. Кроме того, возможность записать равенство $D=P_1A_1+P_2A_2+\ldots+P_nA_n$ уже установлена в пункте 2. Наконец, родство наибольших общих делителей для чисел $A_1, A_2,\ldots, A_n$ следует из теоремы 3.1.4

Замечание. Конечная последовательность нулей обладает наибольшим общим делителем, им является 0. Обозначать наибольший общий делитель гауссовых чисел будем так $\text{ГНОД}(A_1,A_2,\ldots,A_n)$. Далее, заметим, что на гауссовы числа переносятся практические приёмы из § 3 части 1 (естественно, вместо наименьшего натурального числа нужно рассматривать гауссово число с наименьшей нормой).

Определение. Гауссовы числа $A_1,A_2,\ldots,A_n$ назовём взаимно простыми, если $\text{ГНОД}(A_1,A_2,\ldots,A_n)=1$.

Теорема 3.2.2. Пусть $A_1,A_2,\ldots,A_n$, B – гауссовы числа, причём $\text{ГНОД}(A_1,B) = \text{ГНОД}(A_2,B) =\ldots=\text{ГНОД}(A_n,B) =1$. Тогда $\text{ГНОД}(A_1\cdot A_2\cdot\ldots\cdot A_n, B)=1$.

Доказательство повторяет доказательство теоремы 1.3.2 .

Теорема 3.2.3. Пусть AB делится на C, причём A и C – взаимно простые гауссовы числа. Тогда B делится на C.

Доказательство повторяет доказательство теоремы 1.3.3 .

§ 3. Простые гауссовы числа. Основная теорема арифметики для целых гауссовых чисел.

Определение. Гауссово число назовём (гауссовым) простым, если у него имеется ровно два гауссовых делителя (1 и само число), не считая их родственников.

Теорема 3.3.1. Если норма гауссова числа – простое натуральное число, то и гауссово число является (гауссовым) простым числом.

Доказательство. Пусть A – гауссово число и $\|A\|= p$ – простое натуральное число. Если допустить, что A⋮B и $1<\|B\|<\|A\|$, то получим, что p⋮$\|B\|$, а это противоречит тому, что p – простое натуральное число.

Примеры. $2+i$, $-5+8i$ – простые гауссовы числа. $2=(1+i)(1-i)$ – разложение (гауссова) составного числа 2 в произведение (гауссовых) простых чисел.

Теорема 3.3.2 (Основная теорема арифметики для гауссовых чисел). Для каждого гауссова числа, отличного от 0, существует единственное разложение в произведение (гауссовых) простых множителей (с точностью до перестановки сомножителей и с точностью до родственников).

Доказательство (повторяет доказательство теоремы 1.4.3). 1) Если P – гауссово простое число и K – произвольное гауссовое число, то ГНОД(K, P)=1 или ГНОД(K, P)= P, т.к. P делится только на 1 и на P. Следовательно, либо K делится на P, либо K и P – взаимно простые (гауссовы) числа. И далее, произведение гауссовых простых чисел, отличных от данного гауссова простого числа P, не делится на P (теорема 3.2.2).

2) Пусть теперь гауссово число K имеет два разложения на гауссовы простые множители: $K=P^i\cdot A=P^j\cdot B$, причём среди гауссовых простых делителей A и B уже не встречается гауссово простое число P. Тогда A и B не делятся на P (пункт 1). Если допустить, что $i<j$, то после сокращения на P^i получим, что A делится на P – противоречие. Аналогичное противоречие получим, если $j<i$. Таким образом, непременно выполняется $i=j$, т.е. в двух разложениях K на гауссовы простые множители гауссово простое число P входит равное число раз. И это верно для любого гауссова простого делителя K.

Теорема 3.3.3. Пусть простое натуральное число $\mathbf{p}$ не является гауссовым простым числом, т.е. можно записать $\mathbf{p} = A_1\cdot A_2\cdot\ldots\cdot A_n$, где $2\le n$ и $1<\|A_1\|$, $1<\|A_2\|$, …,$1<\|A_n\|$. Тогда $\mathbf{n}=2$, A_1 и A_2 – сопряжённые числа, и $\mathbf{p} = \mathbf{a}^2+\mathbf{b}^2$, где $A_1= \mathbf{a}+\mathbf{bi}$. Кроме того A_1 и A_2 – простые гауссовы числа.

Доказательство. Запишем очевидное равенство $\mathbf{p}^2 = \|A_1\|\cdot\|A_2\|\cdot\ldots\cdot\|A_n\|$. Ввиду теоремы 1.4.3, $n=2$ и $\|A_1\|=\|A_2\|= \mathbf{p}$. Полагаем $A_1=\mathbf{a}+\mathbf{bi}$ и $A_2=\mathbf{c}+\mathbf{di}$, тогда $\mathbf{a}^2+\mathbf{b}^2= \mathbf{p}$, $\mathbf{c}^2+\mathbf{d}^2= \mathbf{p}$ и НОД($\mathbf{a}$, $\mathbf{b}$)=НОД($\mathbf{c}$, $\mathbf{d}$)=1. Следовательно, A_1 и A_2 – сопряжённые числа (теорема 3.1.3). A_1 и A_2 – простые гауссовы числа согласно теореме 3.3.1.

Следствие 1. Простые натуральные числа вида $4k+3$ являются простыми гауссовыми числами.

Доказательство. Для произвольных целых чисел $\mathbf{a}$ и $\mathbf{b}$ остаток от деления $\mathbf{a}^2+\mathbf{b}^2$ на 4 может быть равен 0, 1, 2, но никогда не может быть равен 3. Остаётся применить теорему 3.3.3.

Теорема 3.3.4. Простые натуральные числа вида $\mathbf{4k}+1$ не являются простыми гауссовыми числами. Но каждое из них может быть записано единственным образом в виде $\mathbf{a}^2+\mathbf{b}^2$ ($\mathbf{a}$,$\mathbf{b}$ – натуральные числа) и разложено в произведение двух гауссовых простых, сопряжённых чисел.

Доказательство. Пусть $\mathbf{p}=\mathbf{4k}+1$ – простое натуральное число. По теореме 1.4.5 число $1\cdot2\cdot3\cdot\ldots\cdot(\mathbf{p}-2)\cdot(\mathbf{p}-1)+1$ делится на $\mathbf{p}$. Следовательно, произведение $1\cdot2\cdot3\cdot\ldots\cdot(\mathbf{p}-2)\cdot(\mathbf{p}-1)$ даёт остаток $\mathbf{p}-1$ при делении на $\mathbf{p}$. Запишем иначе это произведение: $1\cdot2\cdot3\cdot\ldots\cdot(\mathbf{p}-2)\cdot(\mathbf{p}-1)=$ $=(1\cdot(\mathbf{p}-1))\cdot(2\cdot(\mathbf{p}-2))\cdot\ldots\cdot(\mathbf{k}\cdot(\mathbf{p}-\mathbf{k}))=(\mathbf{p}-1^2))\cdot(2\mathbf{p}-2^2)\cdot\ldots\cdot(\mathbf{kp}-(\mathbf{k})^2)$. Согласно теореме 1.1.2 (пункт 2) разность $(\mathbf{p}-1^2))\cdot(2\mathbf{p}-2^2)\cdot\ldots\cdot(\mathbf{kp}-(\mathbf{k})^2) -(-1^2)\cdot(-2^2)\cdot\ldots\cdot(-(\mathbf{k})^2)$ делится на $\mathbf{p}$. Но тогда и произведение $1^2\cdot2^2\cdot\ldots\cdot(\mathbf{k})^2$ даёт остаток $\mathbf{p}-1$ при делении на $\mathbf{p}$ (теорема 1.2.2). И ещё один вывод: $(1\cdot2\cdot\ldots\cdot(\mathbf{k}))^2+1$ делится на $\mathbf{p}$. Итак, найдено натуральное число $\mathbf{x}$ так, что $\mathbf{x}^2+1$ делится на $\mathbf{p}$.

Допустим, что **p** – простое гауссово число. Тогда одно из чисел (**x**+**i**) или (**x**–**i**) делится на **p**. А так как числа эти сопряжённые, то и второе из них будет делиться на **p**. Но тогда и их разность **2i** делится на **p**. Но это невозможно, т.к. $\mathbf{p} \neq 2$. Таким образом, **p** не является простым гауссовым числом. А тогда по теореме 3.3.3 существуют натуральные числа **a**,**b** такие, что $\mathbf{p}=\mathbf{a}^2+\mathbf{b}^2$. Наконец, единственность чисел **a**,**b** следует из теоремы 3.3.3 и основной теоремы арифметики для гауссовых чисел.

Следствие 2. Простые натуральные числа вида **4k**+1 могут быть единственным образом записаны в виде $\mathbf{a}^2+\mathbf{b}^2$, где **a**,**b** – натуральные числа.

Уже доказано в теореме 3.3.4.

Следствие 3. Простыми гауссовыми числами являются 1) числа вида **a**+**bi**, где $\mathbf{a}^2+\mathbf{b}^2=2$ или $\mathbf{a}^2+\mathbf{b}^2$ – простое число вида 4k+1 и 2) все простые числа вида 4k+3.

Доказательство. Пусть **a**+**bi** – гауссово простое число. Натуральное число $\|\mathbf{a}+\mathbf{bi}\|$ разложим в произведение простых натуральных чисел $\mathbf{p}_1\cdot\mathbf{p}_2\cdot\ldots\cdot\mathbf{p}_n$. Ввиду основной теоремы арифметики для гауссовых чисел и равенства $(\mathbf{a}+\mathbf{bi})\cdot(\mathbf{a}-\mathbf{bi})=\mathbf{p}_1\cdot\mathbf{p}_2\cdot\ldots\cdot\mathbf{p}_n$ заключаем, что **n**=1 или **n**=2, что соответствует пунктам указанным в следствии.