Наибольшая Общая Мера: последние 2500 лет

Алекандр Степанов

Эта лекция была впервые прочитана в 1999 году как Мемориальная Лекция памяти Артура Шофсталя в Ренсселерском Политехническом Институте.

Аннотация

Цель лекции – это убедить слушателя в том, что математика и алгоритмика едины, и что их единство – центральная тема нашей цивилизации. Идея обобщенных алгоритмов не была придумана нами, но имеет древнюю историю.

Изучение математики развивает архитектурный талант – талант организовывать знания, – который необходим программистам. *Начала* Евклида – это замечательный учебник для разработчиков сложных систем.

Знание истории своей дисциплины необходимо ученому, чтобы отличить важное от второстепенного.

Пифагор (570BC - 475BC)

Табличка Плимптон 322

«Он [Пифагор] придавал важнейшее значение изучению арифметики, которую он развил и отделил от среды коммерческого интереса.»

Аристоксен

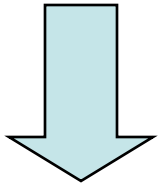
Пифагор учил, что «начала математики – это начала всех вещей».

Аристотель

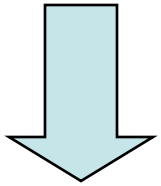
Пифагор развил «теорию иррациональностей и построение небесных тел».

Прокл

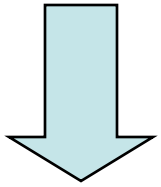
Астрономия



Геометрия



Теория Чисел



Музыка

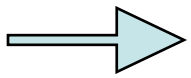
Чтобы свести мир к целым числам, нам нужна единая абсолютная мера, мельчайшее расстояние, квант пространства.

Такой меры нет!

Как бы ни мала была наша мера, есть отрезки, которые она не может измерить.

gcm(a, a) = a

gcm(a, b) = gcm(a, a + b)

a > b  **gcm(a, b) = gcm(a - b, b)**

gcm(a, b) = gcm(b, a)

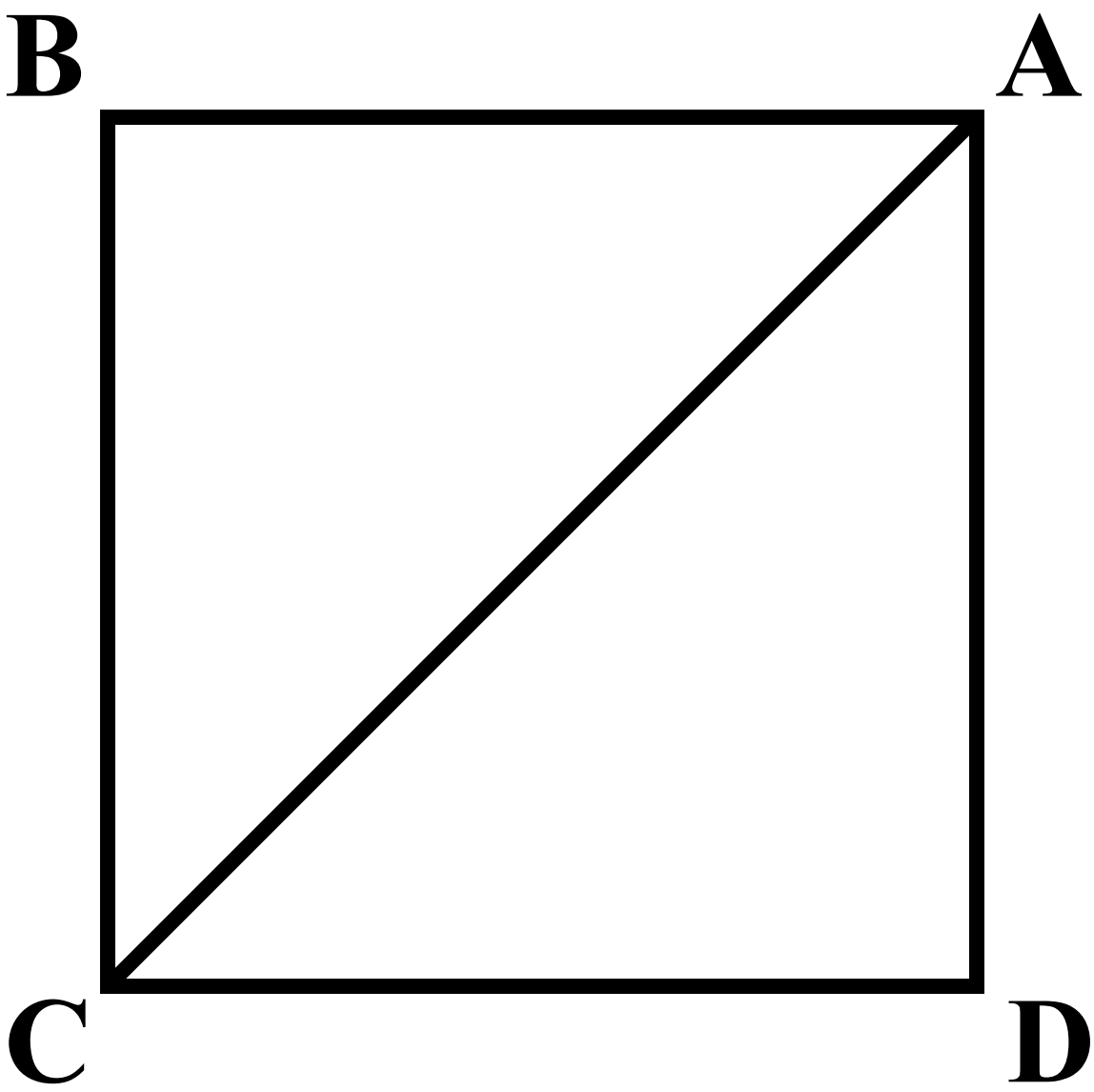
```
line_segment gcm(line_segment a,
                 line_segment b) {
    if (a == b)    return a;
    if (a > b)     return gcm(a-b, b);
    if (a < b)     return gcm(a, b-a);
}
```

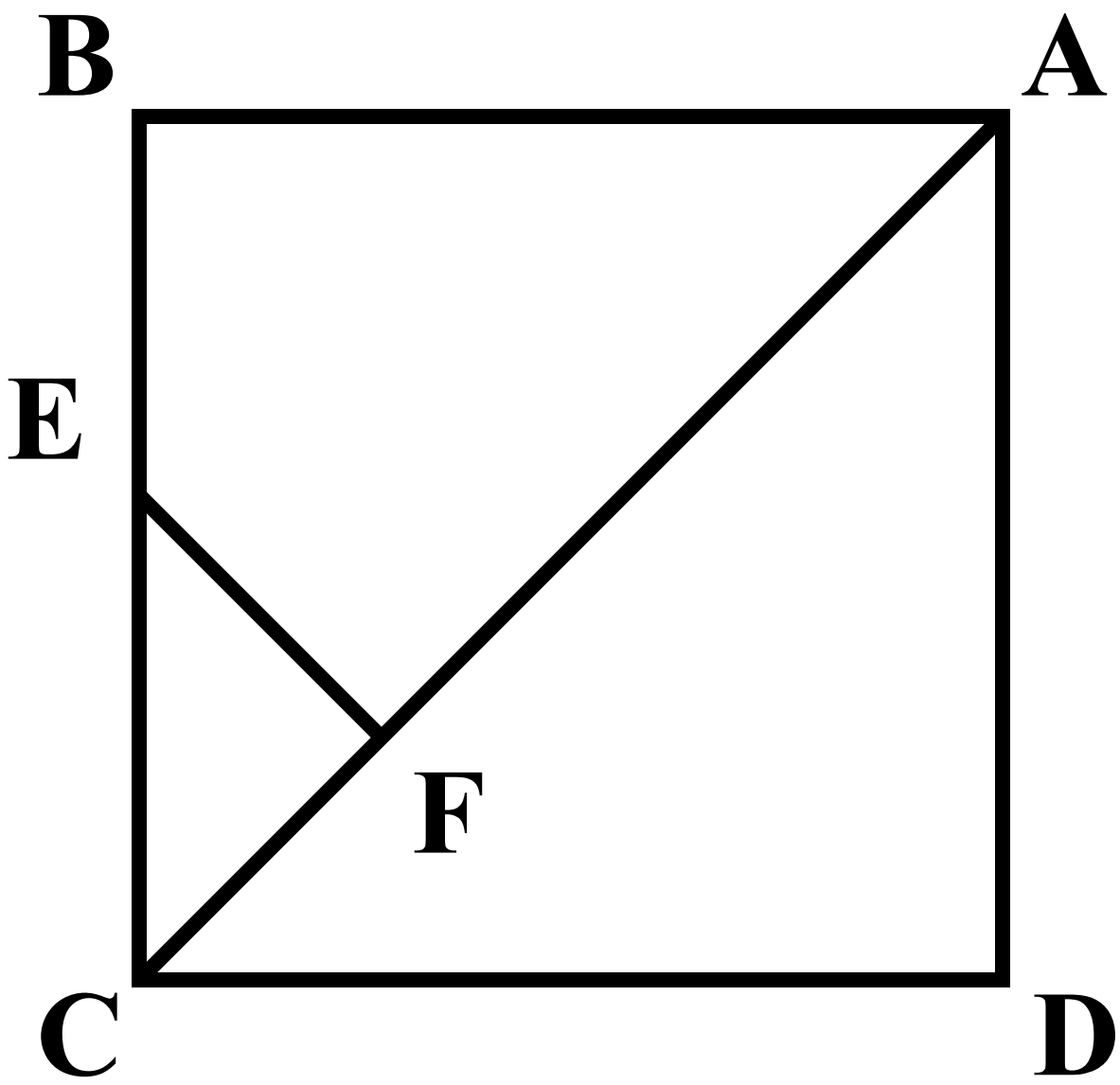
```
196     42
154     42
112     42
 70     42
 28     42
 28     14
 14     14 Done!

GCD:  14
```

Пифагорейцы обнаружили, что всякая нисходящая последовательность натуральных чисел конечна. Это была их форма принципа математической индукции.

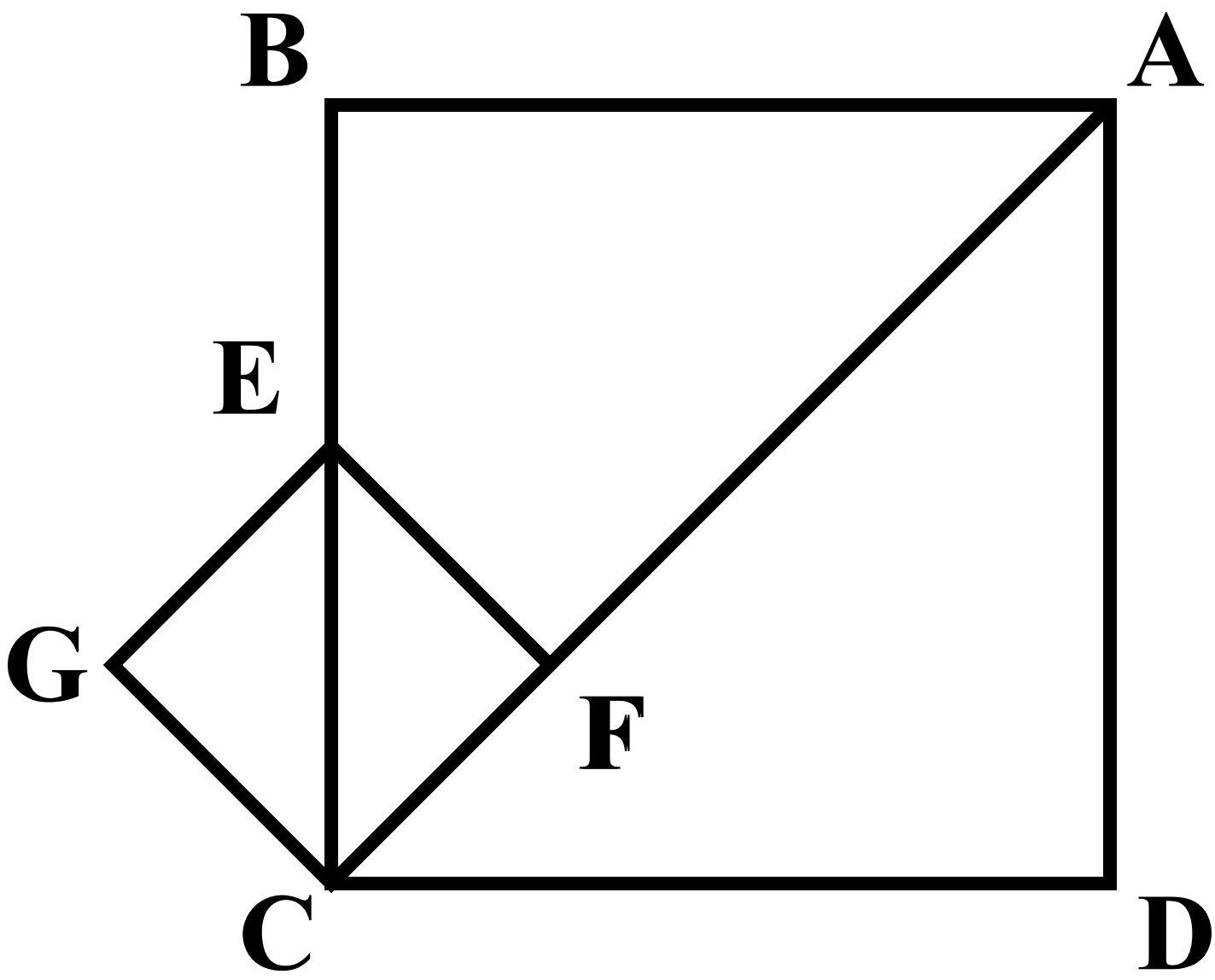
Чтобы доказать, что нечто целочисленное не существует, мы должны показать, что если оно существует, то и нечто меньшее его существует.

Предположим что существует мера, измеряющая сторону и диагональ некоторого квадрата. Теперь возьмем самый малый квадрат, который измеряется этой мерой.

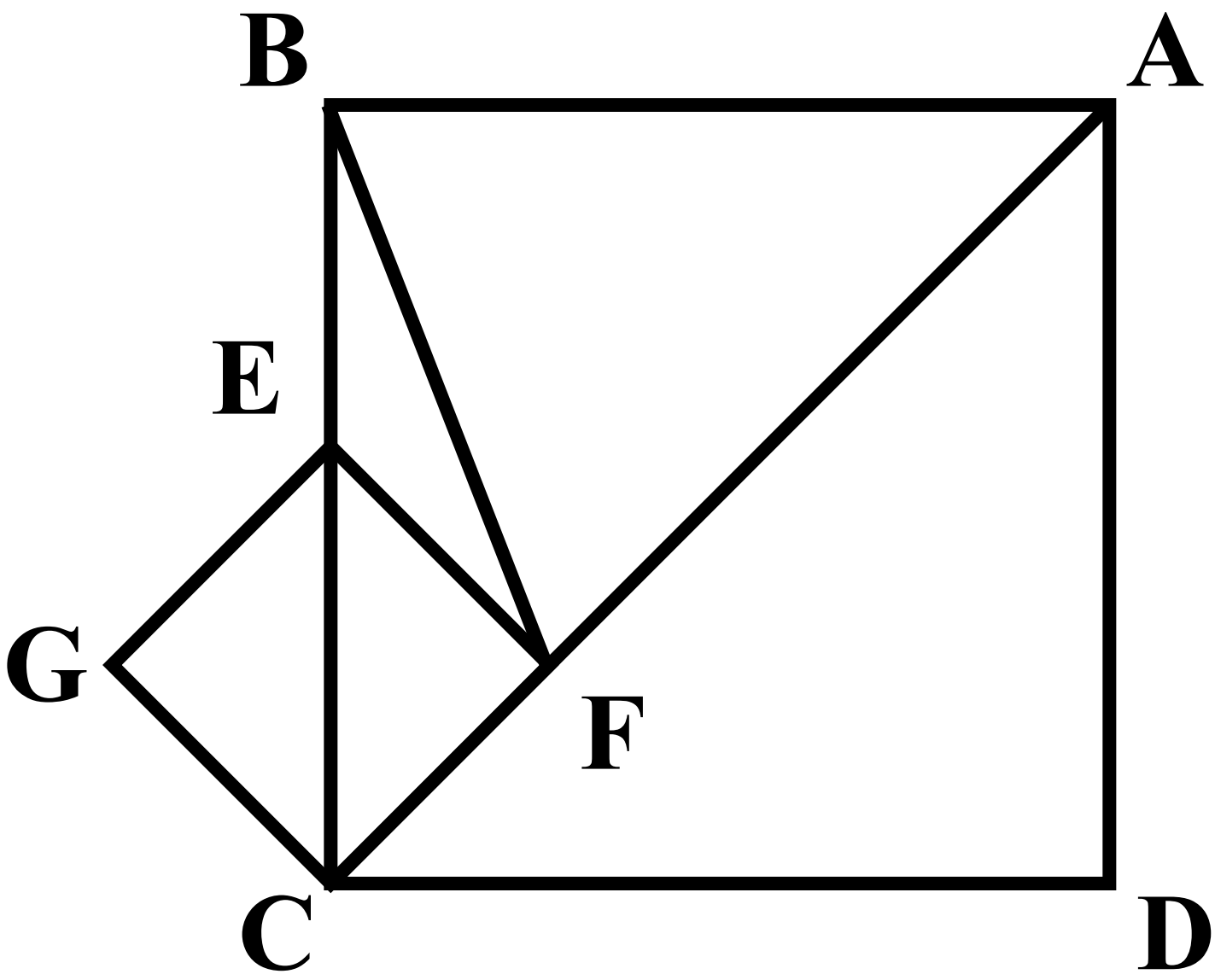

B
A
C
D



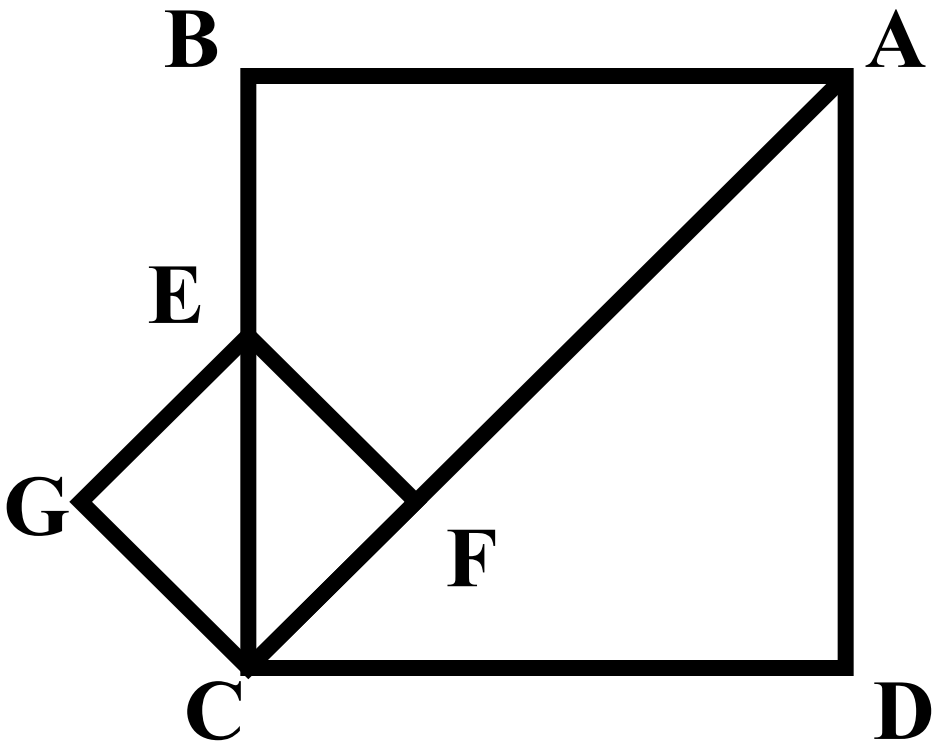
$AB = AF$ $AC \perp EF$



$AC \perp CG$ $EG \perp EF$

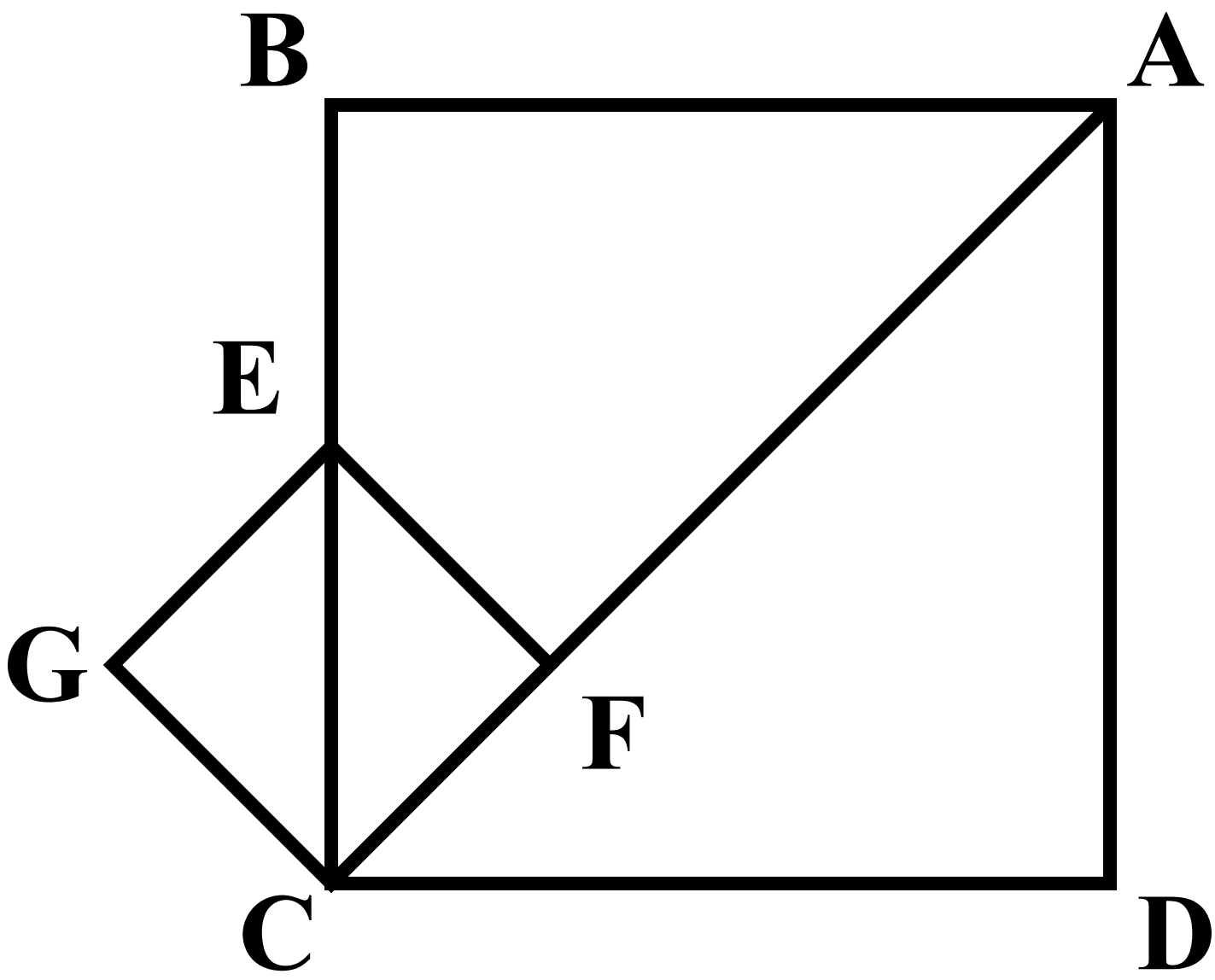


CF = EF = EB



gcm(AC,AB) = gcm(AB,CF)

gcm(CE,CF) = gcm(AC,AB)



$$EC > EB \longrightarrow EB < AB/2$$

Мы построили меньший квадрат, измеряемый этой мерой. Противоречие!

Сторона и диагональ нового квадрата, полученного доказательством, получаются после двух шагов субтрактивного алгоритма:

d, s => s, d - s => 2s - d, d – s

Изначальное отношение между ними сохраняется:

$$d/s = (2s - d)/(d - s)$$

На современном языке, Пифагор открыл, что $\sqrt{2}$ иррационален.

Платон (427BC - 347BC)

ΑΓΕΩΜΕΤΡΗΤΟΣ ΜΗΔΕΙΣ ΕΙΣΙΤΩ

Да не войдет сюда
незнающий геометрии

Они пришли на лекцию Платона о Добре, надеясь, что они узнают, как получить вещи, которые мир называет добром: деньги, или здоровье, или силу. Услышав же, что Платон рассуждал о математике, они были полностью разочарованы.

Аристоксен

Евклид (325BC-265BC)

Некто, начавший изучать геометрию, прошедши первую теорему, спросил Евклида: «Что я заработаю, выучив все это?» Евклид сказал своему рабу: «Дай ему алтын, ибо он хочет от науки поживиться».

Стобей, *Антология*

Евклид гарантирует остановку алгоритма с помощью новых типов переменных:

```
unsigned int gcd(unsigned int a,
                 unsigned int b) {
   assert(a > 0 && b > 0);
   // нужно ждать арабов
   // и Леонардо
Пизанского
   if (a == b)    return a;
   if (a > b)     return gcd(a-b, b);
/* if (b > a) */ return gcd(a, b-a);
}
```

Новая Математика против Евклида

В 1959, на конференции учителей математики во Франции, Жан Дьедонне кричал ”Долой Евклида!” и ”Смерть треугольникам!”

И. М. Яглом *Элементарная Геометрия Прежде и Теперь*

Годы упадка: 212BC - 1202AD

In summo apud illos honore geometria fuit, itaque nihil mathematicis inlustrius; at nos metiendi ratiocinandique utilitate huius artis terminavimus modum.

Среди них [Греков] геометрия была в величайшем почете; ничего не было блистательней математики. Мы [Римляне] ограничили полезность этой науки подсчетами и вычислениями.

Цицерон, *Тускуланские Беседы*

```
if (a > b)      return gcd(a-b, b);
                return gcd(a, b-a);
```

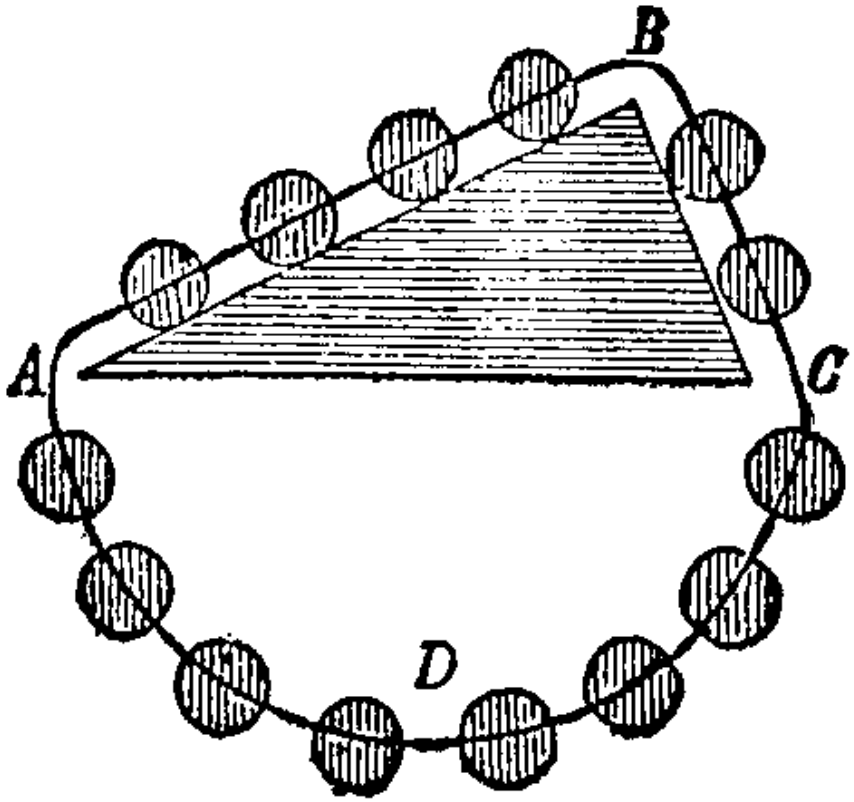
Почему **a-b**, а не **a%b**?

Леонардо Пизанский (1170-1250)

```
unsigned int gcd(unsigned int m,
                 unsigned int n) {
    while (n != 0) {
      unsigned int t = m % n;
      m = n;
      n = t;
    }
    return m;
}
```

```
196     42     196 = 42*4 + 28
 42     28      42 = 28*1 + 14
 28     14      28 = 14*2 + 0
 14     0       Done!

GCD:  14
```

Симон Стевин (1548 - 1620)


B
A
C
D

Симон Стевин:

```
int gcd(int m, int n) {
    while (n != 0) {
      int t = m % n;
      m = n;
      n = t;
    }
    return m;
}
```

Симон Стевин:

```
polynomial<real>
gcd(polynomial<real> m,
    polynomial<real> n) {
   while (n != 0) {
     polynomial<real> t = m % n;
     m = n;
     n = t;
   }
   return m;
}
```

$$
\begin{array}{r|l}
 & 3x^2+2x-2 \\
\cline{2-2}
x-2 & 3x^3-4x^2-6x+10 \\
 & \underline{3x^3-6x^2} \\
 & \quad 2x^2-6x \\
 & \quad \underline{2x^2-4x} \\
 & \qquad -2x+10 \\
 & \qquad \underline{-2x+4} \\
 & \qquad\quad 6
\end{array}
$$

Карл Фридрих Гаусс
(1777 - 1855)

Когда даны числа *A*, *B*, *C* и т.д., их *наибольший общий делитель* находится следующим образом. Пусть все эти числа будут разбиты на простые множители, и из них выберем те, которые являются во всех числах *A*, *B*, *C*, …

...Мы знаем из элементарных соображений, как решить эти проблемы, когда разбиение на простые числа не дано...

Гаусс, *Арифметические Исследования*

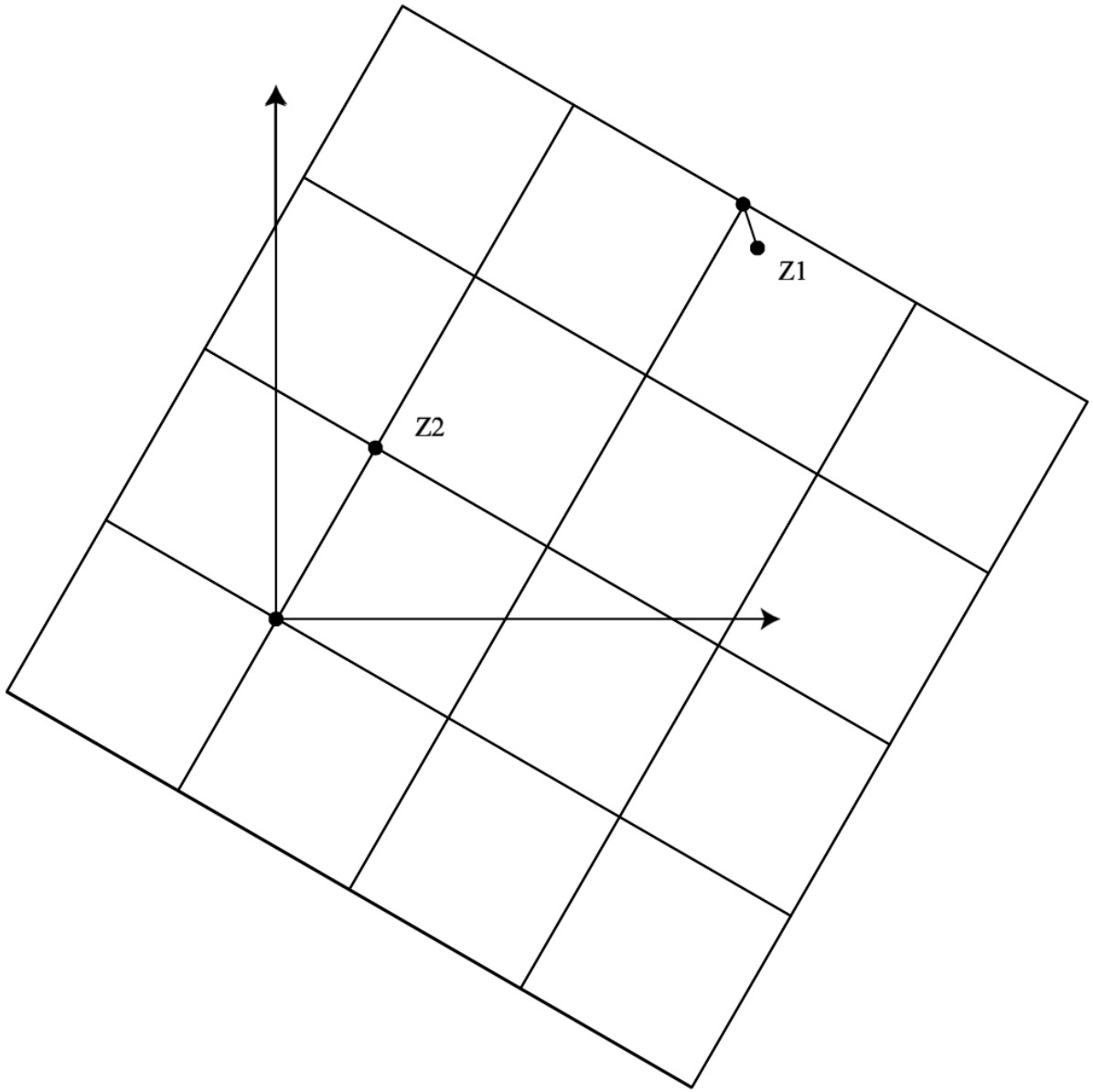
Карл Гаусс:

```
complex<int>
gcd(complex<int> m,
     complex<int> n) {
    while (n != 0) {
      complex<int> t = m % n;
      m = n;
      n = t;
    }
    return m;
}
```

Нахождение остатка от деления двух гауссовых чисел

Чтобы найти остаток от деления `z1` на `z2`

1. Постройте квадратную решетку на комплексной плоскости, порожденную `z2` (вместе с `i*z2`, `-i*z2` и `-z2`).
2. Найдите квадрат в решетке, который включает `z1`.
3. Найдите вершину квадрата `w`, ближайшую к `z1`.
4. Остаток равен `z1 - w`.


Z1
Z2

Петер Густав Лежен Дирихле
(1805 - 1857)

«Теперь нам ясно, что вся структура теории чисел держится на одном основании, именно, на алгоритме для нахождения наибольшего общего делителя двух чисел. Все последующие теоремы … это только элементарные заключения из этого изначального открытия, так что можно утверждать следующее: любая теория, в которой есть подобный алгоритм для наибольшего общего делителя, должна также содержать те же заключения, как и наша теория. И действительно, такие теории существуют!»

Лежен Дирихле
Лекции по Теории Чисел

«Если мы возьмем множество чисел

$$t + n\sqrt{-a}$$

где a – конкретное натуральное число, t и n – произвольные целые числа … то только для некоторых значений of a, например, $a = 1$, наибольший общий делитель двух чисел может быть найден с помощью такого же алгоритма, как и для ... целых чисел. … Это совсем не так, когда $a = 5$. … Например, $21 = 3*7 = (1+2\sqrt{-5})*(1-2\sqrt{-5})$…»

Лежен Дирихле

Лекции по Теории Чисел

Рихард Дедекинд
(1831 - 1916)

Целые алгебраические числа

Целые алгебраические числа – это корни многочленов с целочисленными коэффициентами и с ведущим коэффициентом, равным единице.

Es steht alles schon bei Dedekind!

Эмми Нётер

(Это всё есть у Дедекинда.)

Всё = кольца, поля, идеалы, модули...

Евклид и Геттинген

- Гаусс
  - Правильные многоугольники
  - Пятый постулат
- Дирихле
  - Простые числа в арифметических прогрессиях
- Риман
  - Неевклидова геометрия
- Дедекинд
  - Возрождение теории иррациональностей Евдокса
- Клейн
  - Эрлангенская программа
- Гильберт
  - Основания геометрии
  - Арифметизация математики

Эмми Нётер (1882 -1935)

Если развитие математики сегодняшнего дня несомненно протекает под знаком алгебраизации, проникновения алгебраических понятий и алгебраических методов в самые различные математические теории, то это стало возможным лишь после работ Эмми Нётер.

Павел Сергеевич Александров

Бартель Леендерт ван дер Варден
(1903 - 1996)

Дедекинд, Нётер, ван дер Варден:

```
template <class EuclideanRing>
EuclideanRing gcd(EuclideanRing m,
                  EuclideanRing n) {
    while (n != 0) {
      EuclideanRing t = m % n;
      m = n;
      n = t;
    }
    return m;
}
```

Евклидовы кольца

- Коммутативное кольцо(+, -, *)
- Функция norm: Ring -> Unsigned
  - norm(a*b) >= norm(a)
  - Для всех a, b, где b != 0, существуют q, r, такие что a == q*b + r и
    r == 0 || norm(r) < norm(b)

Дональд Кнут
(1938 -)

Возражение Кнута: **gcd(1, -1) = -1**

```
template <class EuclideanRing>
EuclideanRing gcd(EuclideanRing m,
                  EuclideanRing n) {
    while (n != 0) {
      EuclideanRing t = m % n;
      m = n;
      n = t;
    }
    if (m < 0) m = -m;
    return m;
}
```

Зависит от определения!

Наибольший общий делитель – это делитель, который делится любым другим общим делителем.

Концепция Евклидова кольца

- Операции и их свойства
- Модели
- Алгоритмы

Иосиф Штейн(1961):

```
gcd(n, 0) = gcd(0, n) = n
gcd(n, n) = n
gcd(2n, 2m) = 2gcd(n, m)
gcd(2n, 2m + 1) = gcd(n, 2m + 1)
gcd(2n + 1, 2m) = gcd(2n + 1, m)
gcd(2n + 1, 2(n + k) + 1) =
     gcd(2(n + k) + 1, 2n + 1) =
        gcd(2n + 1, k)
```

```
196          42
 98          21          2
 49          21          2
 28          21          2
 14          21          2
  7          21          2
 14           7          2
  7           7          2    Done!
GCD: 7*2 = 14
```

```
template <class BinaryInteger>
BinaryInteger gcd(BinaryInteger m,
                  BinaryInteger n) {

  make_non_negative(m);
  make_non_negative(n);

  if (is_zero(m)) return n;
  if (is_zero(n)) return m;

  int d = 0;

  while (is_even(m) && is_even(n)) {
    half_non_negative(m);
    half_non_negative(n);
    ++d;
  }
```

```
  while (is_even(m)) half_non_negative(m);

  while (is_even(n)) half_non_negative(n);

  while (true)
    if (m < n) {
      n = n - m;
      do {
        half_non_negative(n);
      } while (is_even(n));
    } else if (n < m) {
      m = m - n;
      do {
        half_non_negative(m);
      } while (is_even(m));
    } else
      return left_shift(m, d);
}
```

Штейн для многочленов

Используй x как 2!

Штейн для многочленов

```
gcd(p,0) = gcd(0,p) = p
gcd(p, p) = p
gcd(x*p1,x*p2) = x*gcd(p1, p2)
gcd(x*p1,x*p2+c) = gcd(p1, x*p2+c)
gcd(x*p1+c,x*p2) = gcd(x*p1+c,p2)
if degree(p1) >= degree(p2)
 gcd(x*p1+c1,x*p2+c2) =
  gcd(p1-(c1/c2)*p2, x*p2+c2)
if degree(p1) < degree(p2)
 gcd(p1,p2) = gcd(p2,p1)
```

x^3-3x-2 x^2-4

$x^3-.5x^2-3x$ x^2-4

$x^2-.5x-3$ x^2-4

x^2-2x x^2-4

$x-2$ x^2-4

x^2-4 $x-2$

x^2-2x $x-2$

$x-2$ $x-2$ Done!

GCD: $x-2$

Алгоритм Вейлерта для гауссовых чисел

Используй 1+i как 2!

Деление на 1+i

$a+bi/1+i = (a+bi)(1-i)/(1+i)(1-i) =$

$(a+bi)(1-i)/2 = ((a+b) - (a-b)i)/2$

Гауссово число $a+bi$ делится на $1+i$ тогда и только тогда $a=b \pmod 2$

Сокращение остатка

Если два гауссовых числа z1 и z2 не делятся на 1+i, то z1+z2, z1-z2, z1+i*z2 и z1-i*z2 делятся на 1+i.

И,

$$\min(|z1+z2|, |z1-z2|, |z1+i*z2|, |z1-i*z2|) < \max(|z1|, |z2|)$$

Алгоритм Damgård и Frandsen

- Алгоритм Штейна также работает для чисел Эйзенштейна Z[ζ], то есть целых чисел, расширенных с ζ ($\frac{-1+\sqrt{-3}}{2}$) (примитивный кубический корень из 1).
- Мы используем 1 – ζ как 2.

Что такое кольцо Штейна?

Неевклидовы кольца Штейна

В 2004 Agarwal и Frandsen показали что есть кольца в которых не работает алгоритм Евклида, но работает алгоритм Штейна.

Заключение

- Информатика это Математика

Библиография

Многие из книг в библиографии существуют в прекрасных русских переводах.

David Fowler, *The Mathematics Of Plato's Academy,* Oxford, 1999

John Stillwell, *Mathematics and Its History*, Springer-Verlag, 1989

Sir Thomas Heath, *History of Greek Mathematics*, Dover, 1981 (2 volumes)

Euclid, *Elements,* translated by Sir Thomas L. Heath, Dover , 1956 (3 volumes)

B. L. van der Waerden, *Geometry and Algebra in Ancient Civilizations*, Springer-Verlag, 1983

Robin Hartshorne, *Geometry: Euclid and Beyond*, Springer-Verlag, 2000

Lucio Russo, *The Forgotten Revolution*, Springer-Verlag, 2004

Laurence E. Siegler, *Fibonacci's Liber Abaci*, Springer-Verlag, 2002

Nicolas Bourbaki, *Elements of the History of Mathematics,* Springer-Verlag, 1999

Carl Friedrich Gauss, *Disquisitiones Arithmaticae,* Yale, 1965

John Stillwell, *Elements of Number Theory*, Springer-Verlag, 2002

Peter Gustav Lejeune Dirichlet, *Lectures on Number Theory,* AMS, 1999

Richard Dedekind, *Theory of Algebraic Integers*, Cambridge, 1996

B. L. van der Waerden, *Algebra*, Springer-Verlag, 1994

Donald Knuth, *Art of Computer Programming, vol. 2, Seminumerical Algorithms*, Addison-Wesley, 1998

Josef Stein, *Computational problems associated with Racah algebra,* J. Comput. Phys., (1967) 1, 397-405

Andre Weilert, *(1+ i)-ary GCD Computation in Z[i] as an Analogue of the Binary GCD Algorithm*, J. Symbolic Computation (2000) 30, 605-617

Ivan Bjerre Damgård and Gudmund Skovbjerg Frandsen, *Efficient algorithms for GCD and cubic residuosity in the ring of Eisenstein integers,* Proceedings of the 14th International Symposium on Fundamentals of Computation Theory, Lecture Notes in Computer Science 2751, Springer-Verlag (2003), 109-117

Saurabh Agarwal, Gudmund Skovbjerg Frandsen, *Binary GCD Like Algorithms for Some Complex Quadratic Rings*. ANTS 2004, 57-71