Unique Factorization and Euclidean Algorithm

Universidad de Cuenca

Optativa 6 - Criptografía

Dr. Diego Ponce

Freddy L. Abad L.
freddy.abadl@ucuenca.edu.ec

Show that $3+\sqrt{10}$ is a divisor of every extended integer of the form $m+n\sqrt{10}$. And extended integer which divides every extended integer is called a unit. All other extended integers is in the system are called no-units (For the ordinary integers, 1 and -1 are the only units). The correct definition of an indivisible in this system of extended integers is an which cannot be written as the product of two non-units.

Basado en el Teorema 1.1

$$\frac{a+b\sqrt{10}}{m+n\sqrt{10}} = \frac{a+b\sqrt{10}}{m+n\sqrt{10}} \times \frac{m-n\sqrt{10}}{m-n\sqrt{10}}$$

Tenemos:

$$\frac{m+n\sqrt{10}}{3+\sqrt{10}} \cdot \frac{3-\sqrt{10}}{3-\sqrt{10}} = \frac{(m+n\sqrt{10})(3-\sqrt{10})}{9-10}$$

$$= \frac{3m+3n\sqrt{10}-\sqrt{10}m-10n}{-1}$$

$$= 10n+m\sqrt{10}-3m-3n\sqrt{10}$$

$$= \underbrace{(10n-3m)}_{\text{integer}} + \underbrace{(m-3n)\sqrt{10}}_{\text{Extended}}$$

1.2 Prove that 2, 3, $4+\sqrt{10}$ and $4-\sqrt{10}$ really are indivisible in the system of extended integers of the form $m+n\sqrt{10}$. Hint: if

$m+n\sqrt{10} = (a+b\sqrt{10}) \times (c+d\sqrt{10})$ then
$m-n\sqrt{10} = (a-b\sqrt{10}) \times (c-d\sqrt{10})$ and so
$m^2-10n^2 = (a^2-10b^2) \times (c^2-10d^2)$

If $a+b\sqrt{10}$ and $c+d\sqrt{10}$ are no units, then in each of these 4 cases

a^2-10b^2 and c^2-10d^2

must be 2, -2, 3, -3 show that any perfect square is a multiple of 5 or 1 more or less than a multiple of 5 and therefore

$a^2-10b^2 = 2, -2, 3, -3$ has no integer solution

2, 3 es un # primo

Teorema 1.1 $\therefore n = p \cdot k$; $n, k, p \in \mathbb{E}$

$n \mid p$, p es primo $\Rightarrow k \mid p$ o $q \mid p$

El numero 2 y 3 son primos por el Teo 1.1, NO TIENEN FACTOR DE DESCOMPOSICION, entonces es indivisible el sistema de enteros extendidos.

Demostración por contradicción

$4+\sqrt{10} = (a+b\sqrt{10})(c+d\sqrt{10})$

$4-\sqrt{10} = (a-b\sqrt{10})(c-d\sqrt{10})$

$16-10 = (a^2-10b^2)(c^2-10d^2)$

$6 = (a^2-10b^2)(c^2-10d^2)$

$2\times 3 \neq (4-\sqrt{10})(4-\sqrt{10})$

∴ Incongruente, es indivisible en el sistema de enteros extendidos

1.3. Prove that the square roots of 3 and 5 cannot be written as rational numbers

TESIS $\sqrt{3}$ es racional

HIPOTESIS a/b es par/impar
p es primo
$\sqrt{p}$ es racional

$\sqrt{3} = \frac{a}{b}$

(a y b no tienen factores comunes excepto el 1

$3 = \frac{a^2}{b^2} \Rightarrow 3b^2 = a^2$

a^2 es multiplo de 3

$a = f_1 f_2 f_3 \cdots f_k$

$a^2 = f_1 f_1 f_2 f_2 \cdots f_k f_k$

3 puede ser algun f_i (f_1 o f_2, etc)

3 es f_2, ∴ 3^2 es f_2^2

∴ a es multiplo de $\sqrt{3}$

$a = 3k$

$3b^2 = a^2$

$3b^2 = (k3)^2$

$3b^2 = k^2 3^2 \Rightarrow b^2 = \frac{k^2 3^2}{3}$

$b^2 = 3k^2$

∴ b^2 es multiplo de 3
b es multiplo de $\sqrt{3}$

∴ INCONSECUENCIA, ya que $\sqrt{3}$ no es racionalmente representable porque a & b no son multiplos por hipotesis

Demostración por contradicción

Caso $\sqrt{5}$

Hipotesis a/b es par/impar
p es primo
$\sqrt{p}$ es racional

$\sqrt{5} = \frac{a}{b}$

a y b no tienen factores comunes por

$5 = \frac{a^2}{b^2} \Rightarrow 5b^2 = a^2$

a^2 es multiplo de 5

$a = f_1 \cdot f_2 \cdots f_n$

$a^2 = f_1 f_1 f_2 f_2 \cdots f_n f_n$

5 puede representarse por un f_n (Ejm: $5 = f_2$)

$\therefore 5 = f_2 \Rightarrow 5^2 = f_2^2$

$\therefore$ a es multiplo de $\sqrt{5}$

$a = 5k$

$5b^2 = a^2$

$5b^2 = (5k)^2$

$5b^2 = 5^2k^2$

$b^2 = \frac{5^2 k^2}{5}$

$b^2 = 5k^2$

$\therefore b^2$ es multiplo de 5

$\therefore$ b es multiplo de $\sqrt{5}$

$\therefore$ INCONGRUENCIA, ya que $\sqrt{5}$ no es racionalmente representable porque a & b no son multiplos por hipótesis

Demostración por contradicción

1.4. Prove that if n is a positive integer which is not the square of another integer then the square root of n cannot be written as a rational number

HIPOTESIS [H.1] $n>0$, $n \in \mathbb{E}$ y n no es la raiz de otro entero

[H.2] $\sqrt{n} = \frac{m}{s}$; $m, s \in \mathbb{E} \Rightarrow m, s$ no tienen un divisor común a parte de 1

$(\sqrt{n})^2 = (\frac{m}{s})^2$

$n = \frac{m^2}{s^2}$

$ns^2 = m^2$; 2 es un factor

$ns^2 = m^2 \wedge [H.1] \Rightarrow n|m^2$ Teorema 1.1 $\Rightarrow 2n = m^2 \wedge 2n|ns^2$ [H.3]

$[H.1] \wedge [H.2] \wedge [H.3] \Rightarrow n|s^2 \wedge$ Teorema 1.1

L.Q.Q.D.

Por contradicción, debido a n puede ser dividido con m y s. m y s no tienen factores comunes aparte de 1 [H.1]

1.5 Find all fundamental Pythagorean triples (x, y, z) with x, y less 50

El numero de Pythagorean triples menor que un n esta dado por la formula

$$\tilde{T}(n) = \frac{4 \log(1+\sqrt{2})}{\pi^2} n \log n$$

$n = 50$

$\hat{T}(n) = 16$

$$\frac{4 \log(1+\sqrt{2})}{\pi^2}(50) = 18$$

$\check{T}(n) = 52$

$$\frac{4 \log(1+\sqrt{2})}{\pi^2}(50) \log(50) = 70$$ //

find all that, if a and b are relatively prime, $a > b > 0$, and one is odd, that other even, then

$$(a^2 - b^2,\ 2ab,\ a^2 + b^2)$$

is a fundamental triple.

1.7 Show that if x, y, z is postive integer which satisfy

$$x^2 + 2y^2 = z^2$$

and they have no common diuser, then there exist relatively prime integers a & b where b is odd such that

$$x = |2a^2 - b^2|$$

$$y = 2ab$$

$$z = 2a^2 + b^2$$

1.8 To say that d divides a means that there is on integer m such that $a = d \times m$. Prove that the Fundamental theorem of Arithmetics implies Teo 1.1

Using Euclides Algorithm find gcd (31408, 2718)

gcd (31408, 2718)

31408	2718
-29898	11
1510	

→

2718	1510
1510	1
1208	

1510	1208
1208	1
0302	

1208	302
0	4

∴ gcd = 302 //

1.10 Let lcm(a,b) denotate the least common multiple of a & b Prove that lcm(a,b) = (a×b) /gcd(a,b)

lcd(a,b)·gcd = a×b

① m = lcd(a,b) y d = gcd(a,b)

md = ab y → Reemplazo

a|m = b|m ⇒ md = ab

$m = \frac{ab}{d}$

m = qμ

$\frac{ab}{d} = q\mu$

$\frac{b}{d} = \mu$

μ = bv

m = qμ

m = abv

b|m = b|aqμ

⇒ b|a o b|μ ab|m //

∴ ab es menor igual que cualquier multiplo común de a & b

② El $lcd(\frac{a}{d}, \frac{b}{d}) = \frac{m}{d}$

$\frac{a}{d}|k$ y $\frac{b}{d}|k$ ⇒ a|kd y b|kd

Luego m|kd ⇒ $\frac{m}{d}|k$

Entonces $\frac{m}{d}$ es el menor multiple comun de $\frac{a}{d}$ y $\frac{b}{d}$

Respuesta: $\frac{m}{d} = \frac{a}{d} \cdot \frac{b}{d}$

$\frac{md^2}{d} = ab$ md = ab

m = lcd(a,b) d = gcd(a,b)

∴ lcd(a,b) gcd(a,b) = ab

- d es divisor de a & b
- d es dividido por cualquier divisor de a & b

∴ d es gcd

1.11 Implement Alg 1.7 and test on:

(A) (31408, 2718)

(B) (21 377 104, 12 673 234)

(C) (355 876 536, 319 256 544)

(D) (64187 85375, 78499 11069)

Algoritmo 1.7: Algoritmo Euclide para encontrar gcd/mcd.

```
public long gcdEuclides(long a, long b)
{
    while(b!=0){
        long temp=b;
        b=a%b;
        a=temp;
    }
    return a;
}
}
```

Pruebas:

(A) gcdEuclides(31408, 2718) = 302

(B) gcdEuclides(21 377 104, 12673 234) = 434

(C) gcdEuclides(355 876 536, 319 256 544) = 456

(D) gcdEuclides(64187 85375, 78499 11069) = 1001

Show that if the absolute value of a is less that the absolute value of b, then the FIRST ITERAT. of DIVISION_ loop of Alg 1.7 reverse the order of these values.

#Iteraciones	a	b	b≠0	temp=b	b=a %b	a=temp
1	18	12	False	12	6	12
2	12	6	False	6	1	6
3	6	1	False	1	0	1
4	1	0	True			

El orden de los valores a & b se invierten en la primera iteracion.

1.13. Analyse what happens in Alg 1.7 if a &/or b is −.
(Note: Replacing v by −v does not change the value of v MOD

a = 5
b = −2

5 mod −2 = 1

5	−2
1	−2

−2	1
0	−2

∴ Si a y/ó b son negativos, entonces el valor absoluto del valor final de a sigue siendo el mayor divisor común

Prove that if m is an int, then the set of common divisors of b and a-mb, and this

$$gcd(a,b) = gcd(b, a-m\times b)$$

HIPOTESIS: m es entero

TESIS $gcd(a,b) = gcd(b, a-mb)$

1.15 Write a program that implement Alg. 1.8 and test on the pairs of exeras 1.1.

```
public long gcd (long u, long v);
        if(u==v)
            return u;
        if (u==0)
            return v;
        if(v==0)
            return u;
        if(~u&1)
        {
            if(v&1)
                return gcd(u>>1, v)
            else
                return gcd(u>>1, v>>1)<<1;
        }
        if(~v&1)
            return gcd(u, v>>1)
        if (u>v)
            return gcd((u-v)>>1, v)
        return gcd((v-u)>>1, u);
    }
```

(A) gcd(31408, 2718) = 302

(B) gcd(21377 1045 1267 3234) = 434

(C) gcd(355876536, 319255441) = 456

(D) gcd(841878535, 7849911069) = 1001

In Alg 1.8 verify that after each iteration of DIVISION_LOOP the equation

$$u_3 = u_1 \times a + u_2 \times b$$
$$v_3 = v_1 \times a + v_2 \times b$$

are still satisfied.

$a = 1239$
$b = 168$

$u_1 = 1$
$u_2 = 0$
$u_3 = 168$

$v_1 = 1$
$v_2 = 0$
$v_3 = 1239$

ITERACION	u_1	u_2	u_3	$au_1 + bu_2$	condicion	cumple
1	1	0	168	1239(1)+168(0)	$168 \neq 1239$	False
2	-6	0	63	1239(-6)	$63 \neq -7439$	False
3	13	0	42	1239(13)	$42 \neq 16107$	False
4	-19	0	21	1239(-19)	$21 \neq -23541$	False

Valores de v

ITERACION	v_1	v_2	v_3	$av_1 + bv_2$	condicion	cumple
1	-6	0	63	1239(-6)+168(0)	$63 \neq -7434$	False
2	13	0	42	1239(13)	$42 \neq 16107$	False
3	-19	0	21	1239(-19)	$21 \neq -23541$	False
4	51	0	0	1239(51)	$0 \neq 63189$	False

∴ NO CUMPLEN CONDICIONES

1.17 What are the values of v_1 and v_2 when Alg 1.8 terminates?

$v_1 = 9/2$

$v_2 = 5/2$

1.18 Find 2 other integral solution to the equation

$$1239xm + 168xn = 21$$

1.19 Show that there are infinitely many integral solution of

$$1239xm + 168xn = 21$$

Describe how they are generated

Write a program for Alg 1.4 and test with pairs of Exercise 1.11

```
public int gcd(int u, int v){
  int shift;
  if (u==0)
      return v;
  if (v==0)
      return u;

  for(shift=0; ((u|v)&1)==0; ++shift)
  {
      u>>=1;
      v>>=1;
  }
  while((u&1)==0)
      u>>1;
  do
  {
    while((v&1)==0)
        v>>1;
    if (u>v)
    { int t=v;
      v=u;
      u=t;
    }
    v=v-u;
  }while(v!=0);
    return u<<shift;
};
```

(A) gcd(31408; 2718) = 302

(B) gcd(21377104, 12673234) = 434

(C) gcd(355876536, 319256544) = 456

(D) gcd(841877375, 749911069) = 1001

1.21 Prove that Alg 1.9 will eventualy terminate

(A) gcd(31408, 2718) = 302

(B) gcd(21377 104, 12 673 234) = 434

(C) gcd(355 876 536, 319 256 544) = 114

(D) gcd(84187 85375, 78499 11069) = 1001

El Algoritmo termina siempre y cuando se agregue una condicion en el metodo redice que si r=0 entonces salga del bucle, condición la cual fue agregado en la pregunta 1.10

1.22 Base teo 1.10 Hint: Start by rewritten the sucessive equalities of Euclidean Alg. as

$$a/b = m_1 + r_1/b$$

$$b/r_1 = m_2 + r_2/r_1$$

$$r_1/r_2 = m_3 + r_3/r_2$$

$$\vdots$$

$$r_{k-2}/r_{k-1} = m_k + r_k/r_{k-1}$$

$$r_{k-1}/r_k = m_{k+1}$$

$$\begin{array}{c|c} a & b \\ r_1 & m_2 \end{array}$$

$a = bm + r_1 \rightarrow r_1 = a - bm$

$b = r_1 m_2 + r_2 \rightarrow r_2 = r_3 m_3 + r_3$

$r_2 = b - r_1 m_2$ //

Unique Factorization and Euclidean Algorithm

Universidad de Cuenca

Optativa 6 - Criptografía

Dr. Diego Ponce

Freddy L. Abad L.
freddy.abad@ucuenca.edu.ec