Basic Math - Second lesson

Caboara

1 Greater Common Divisor - $\mathbb{N}$

Definition 1. *If $a, b \in \mathbb{N}$, the greater common divisor of a, b is the biggest $p \in \mathbb{N}$ such that $p|a$ and $p|b$. Since $1|a$ and $1|b$, if there are no other common divisor,* $\gcd(a, b) = 1$*.*

Remark 2. *If $a, b \in \mathbb{N}$ a divides $b \Leftrightarrow$ exists $c \in \mathbb{N}$ such that $b = c \cdot a$. We write*

$$a|b \Leftrightarrow \exists\ c \in \mathbb{N} \textit{ such that } b = c \cdot a$$

Since for every $a \in \mathbb{N}$ $0 = 0 \cdot a$, we have that 0 is divisible by any natural number. Hence, $\gcd(a, 0) = a$

Computing GCD's using factorizations.

Proposition 3. *If we have $a, b \in \mathbb{N}$ and their prime factorization*

$$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n} q_1^{\gamma_1} \cdots q_m^{\gamma_m} \qquad \textit{and} \qquad a = p_1^{\beta_1} \cdots p_n^{\beta_n} s_1^{\theta_1} \cdots s_t^{\theta_t}$$

(the p_i are the common prime factors) then

$$\gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdots p_n^{\min(\alpha_1, \beta_1)}$$

We can say that the greatest common divisor of a and b, if their prime factorizations are known, is the product of the common prime factors, taken with the minimum exponent.

Example 4.

1. *Since* $600 = 2^3 \cdot 3 \cdot 5^2$ *and* $252 = 2^2 \cdot 3^2 \cdot 7$ *we have that* $\gcd(600, 252) = 2^2 \cdot 3 = 12$.
2. *Since* $70 = 2 \cdot 5 \cdot 7$ *and* $429 = 3 \cdot 11 \cdot 3$ *we have that* $\gcd(70, 429) = 1$.

The greatest common divisor has the following properties

Proposition 5. *If $a, b, c \in \mathbb{N}$*

1. $\gcd(a, b) = \gcd(b, a)$.
2. $\gcd(a, a) = a$.
3. $\gcd(a, 0) = a$.

4. $\gcd(0,0)$ *is undefined. Why?*

5. $\gcd(ac, bc) = c\gcd(a,b)$.

6. *If* $a = cb+r$, *with* r *the remainder of the division of* a *by* b *we have* $\gcd(a,b) = \gcd(cb+r, b) = \gcd(r,b) = \gcd(b,r)$.

Computing GCD's using Euclid's Algorithm.

Example 6. *Using the rule* $\boxed{\gcd(a,b) = \gcd(b,r)}$ *with* r *the remainder of* a *divided by* b. *We compute some* gcd *using the* `EuclidVerbose` *procedure of CoCoA.*

1. `EuclidVerbose(15,12);`
```
[15, 12]
[12, 3]
[3, 0]
GCD(15,12)=3
3
```

2. `EuclidVerbose(2343,432);`
```
[2343, 432]
[432, 183]
[183, 66]
[66, 51]
[51, 15]
[15, 6]
[6, 3]
[3, 0]
GCD(2343,432)=3
3
```

3. `EuclidVerbose(347,237);`
```
[347, 237]
[237, 110]
[110, 17]
[17, 8]
[8, 1]
[1, 0]
GCD(347,237)=1
1
```

Definition 7. *If* $a, b \in \mathbb{N}$ *and* $\gcd(a,b) = 1$ *we say that* a, b *are* coprime. *Coprime natural numbers have no common divisors other than* 1. *A prime number* p *is coprime with every natural number except its multiples, i.e., numbers of the form* p^n.

Remark 8. *We remark that if* $c \in \mathbb{N}$ *is coprime with* $b \in \mathbb{N}$ *then* $\gcd(ac, b) = \gcd(a,b)$. *We can discard coprime factors.*

1. $\gcd(32 \cdot 5, 27) = \gcd(32, 27)$ *since* $5, 27$ *are coprime.*

2 Greater Common Divisor - Polynomials

Definition 9. *An polynomial $p(x) \in \mathbb{R}[x]$ is* irreducible *if there is no other polynomial $f(x) \in \mathbb{R}[x]$ of degree bigger or equal to 1 that divides $p(x)$. A polynomial is* reducible *if it is not irreducible. itself. Irreducible polynomials play the role of prime numbers.*

Example 10.

1. *All degree one polynomials are irreducible.*
2. *A polynomial $ax^2 + bx + c$ is irreducible if and only if $\Delta = b^2 - 4ac > 0$.*
3. *$x^2 + x + 1$ is irreducible since $\Delta = 1 - 4 < 0$.*
4. *$x^2 + 1$ is irreducible since $\Delta = 0 - 4 < 0$..*
5. *A polynomial $ax^2 + bx + c$ is reducible if and only if $\Delta = b^2 - 4ac \leq 0$.*
6. *The polynomial x^2-5x+6 is reducible because $(x-2)|(x^2-5x+6)$. Also $\Delta = 25-24 = 1 > 0$.*
7. *The polynomial $4x^2-12x+9$ is reducible because $(2x-3)|(4x^2-12x+9)$. Also $\Delta = 144-144 = 0$.*
8. *The polynomial $p(x) = x^4-3x^3+5x^2-9x+6$ is reducible since $p(x) = (x-1)(x-2)(x^2+3)$.*
9. *Find if a polynomial of degree ≥ 3 is reducible or not can be quite difficult.*

Remark 11. *All the properties of the GCD over the natural numbers hold for the polynomials. Moreover by convention, the GCD of polynomials is defined not taking into consideration purely numeric factors. Hence, we can take out of the computations any pure number, not only coprime factors.*

$$F(x), G(x) \in \mathbb{R}[x],\ a \in \mathbb{R}, \quad \gcd(F(x), aG(x)) = \gcd(F(x), G(x))$$

We have $\gcd(2x^2, 4x) = x$, *and*

$$\begin{aligned} \gcd((x-2)(3x-3), x^2-1) &= \gcd(3(x-2)(x-1), x^2-1) \\ &= \gcd((x-2)(x-1), x^2-1) \\ &= \gcd((x-2)(x-1), (x+1)(x-1)) \\ &= x-1 \end{aligned}$$

We can compute Polynomial GCD's easily if we know the irreducible factorization, at least of one factor

Example 12. *The polynomials $x-2, x-7, x-1$ are irreducible since they have degree one. The polynomial x^2+2 is irreducible since it has negative Δ.*

$$\gcd((x-2)^2(x^2+2)^3(x-7), (x-2)(x^2+2)^4(x-1)) = (x-2)^{\min(2,1)}(x^2+2)^{\min(3,4)} = (x-2)(x^2+2)^3$$

Example 13. *We have to compute* $\gcd(x^4+x-7, x^2-1)$. *We define* $p(x) = x^4+x-7$ *and we note that irreducible factorization* $x^2-1 = (x+1)(x-1)$, *so*

$$\gcd(x^4+x-7, x^2-1) = \gcd(x^4+x-7, (x+1)(x-1))$$

the GCD has to have the common factors, but there are none, since

$$p(1) = -5 \Rightarrow (x-1) \nmid p(x) \quad \text{and} \quad p(-1) = -7 \Rightarrow (x+1) \nmid p(x)$$

Hence, $\gcd(x^4+x-7, x^2-1) = 1$ *and* $x^4+x-7,\ x^2-1$ *are coprime.*

We can use Euclid's Algorithm for the GCD in the polynomial case, using polynomial divisions.

The computations are done using the `GCDPolyVerbose` command of the CoCoA system. The remainder sequence for $f(x),\ g(x)$ is given by $f(x),\ g(x)$ and the remainders, if suitable regrouping and taking out numeric factors

Example 14.

```
GCD(x^2+x+1,x^2+2)=
We divide x^2+x+1 by x^2+2, the remainder is x - 1
(x^2 + x + 1)=(1)*(x^2 + 2)+(x - 1)

=GCD(x^2+2,x - 1)=
(x^2 + 2)=(x + 1)*(x - 1)+(3)
We divide x^2+2 by x-1, the remainder is 3

=GCD(x - 1,3)=GCD(x - 1,1) (we took out the number 3)

=GCD(x - 1,1)=1 there is no common factor

The remainder sequence is x^2 + x + 1, x^2 + 2, x - 1, 1
```

Example 15.

```
GCD(x^4+x^3-1,x^3+x-2)=
(x^4 + x^3 - 1)=(x + 1)*(x^3 + x - 2)+(-x^2 + x + 1)
We divide x^4+x^3-1 by x^3+x-2 the remainder is -x^2 + x + 1

=GCD(x^3+x-2,-x^2 + x + 1)=
(x^3 + x - 2)=(-x - 1)*(-x^2 + x + 1)+(3x - 1)
We divide x^3+x-2 by -x^2 + x + 1 the remainder is 3x - 1

=GCD(-x^2 + x + 1,3x - 1)=
(-x^2 + x + 1)=(-1/3x + 2/9)*(3x - 1)+(11/9)
We divide -x^2 + x + 1 by 3x - 1 the remainder is 11/9
```

```
=GCD(3x - 1,11/9)=GCD(3x - 1,1)=1 We took out the numeric factor 11/9

The remainder sequence is x^4 + x^3 - 1, x^3 + x - 2, -x^2 + x + 1, 3x - 1, 1
```

Example 16.

```
GCD(x^4 - 6x^3 + 7x^2 + 12x - 18,x^3 + x^2 - 2x - 2)=
(x^4 - 6x^3 + 7x^2 + 12x - 18)=(x - 7)*(x^3 + x^2 - 2x - 2)+(16x^2 - 32)
We divide x^4 - 6x^3 + 7x^2 + 12x - 18 by x^3 + x^2 - 2x - 2,
the remainder is 16x^2 - 32=16(x^2-2)
We take out the number 16, the remainder is now x^2-2

=GCD(x^3 + x^2 - 2x - 2,x^2-2)=
(3x^3 + 2x^2 - 6x - 4)=(-3x - 2)*(-x^2 + 2)+(0)
We divide x^3 + x^2 - 2x - 2 by x^2-2, the remainder is 0

=GCD(x^2-2,0)=x^2-2

The remainder sequence is x^4 - 6x^3 + 7x^2 + 12x - 18, x^3 + x^2 - 2x - 2, x^2 - 2
```

3 Derivative for polynomials

Definition 17. *If* $f(x) = a_n x^n + a_{n-1}a^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$ *the* derivative *of* $f(x)$ *or* $D(f(x))$ *or* $f'(x)$ *is*

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 + 0$$

Note that since for $a \in \mathbb{R}$, $a = a \cdot x^0$, $(a)' = 0$

Example 18.

$$(x^5 - 3x^2 + x - 2)' = 5x^4 - 6x + 1$$

$$(3x^7 - 3x^5 + x^3 + 1)' = 21x^5 - 15x^4 + 3x^2$$

Proposition 19. *It is easy to prove that, for* $f(x), g(x) \in \mathbb{R}[x]$

1. $(f(x) + g(x))' = f'(x) + g'(x)$.
2. $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$.
3. $(f(x)^n +)' = n \cdot f(x)^{n-1} \cdot (f'(x))$.

Example 20.

$$\begin{aligned}((3x^2-2)(x^2+x+1))' &= (3x^2-2)'(x^2+x+1) + (3x^2-2)(x^2+x+1)' \\ &= (6x)(x^2+x+1) + (3x^2-2)(2x+1) \\ &= 12x^3 + 9x^2 + 2x - 2\end{aligned}$$

If we do the computations and then derive, we have

$$((3x^2-2)(x^2+x+1))' = (3x^4+3x^3+x^2-2x-2)' = 12x^3+9x^2+2x-2$$

Example 21.

$$\begin{aligned}((x^2+2x-1)^3)' &= 3(x^2+2x-1)^2(x^2+2x-1)' \\ &= 3(x^2+2x-1)^2(2x+2) \\ &= 6x^5+30x^4+36x^3-12x^2-18x+6\end{aligned}$$

If we do the computations and then derive, we have

$$((x^2+2x-1)^3)' = (x^6+6x^5+9x^4-4x^3-9x^2+6x-1)' = 6x^5+30x^4+36x^3-12x^2-18x+6$$

4 Multiple factors

Proposition 22. *If $f(x) \in \mathbb{R}[x]$ and $\gcd(f(x), f'(x)) = p(x)$ then $p(x) \mid f(x)$. If $p(x)$ is irreducible, then $p(x)^2 \mid f(x)$.*

Definition 23. *If $\gcd(f(x), f'(x)) = 1$ we say that $f(x)$ is* squarefree*, e.g. there are no multiple factors in its irreducible factorization.*

Remark 24. *If $f(x) \in \mathbb{R}[x]$, we have that $\frac{f(x)}{\gcd(f(x),f'(x))}$ is squarefree.*

Example 25. *Let $p(x) = x^4-4x^3+6x^2-8x+8$; We have that (do the GCD as an exercise)*

$$\gcd(p(x), p'(x)) = x-2$$

That means that, since $x-2$ is irreducible, $(x-2)^2 \mid (x^4-4x^3+6x^2-8x+8)$. Indeed, we have

$$\frac{x^4-4x^3+6x^2-8x+8}{x^2-4x+4} = x^2+2$$

Hence, $x^4-4x^3+6x^2-8x+8 = (x^2+2)(x-2)^2$.

Example 26. *Let $p(x) = x^6+8x^5+2x^4-36x^3+x^2+52x-28$; We have that (do the GCD as an exercise)*

$$\gcd(p(x), p'(x)) = x^3-3x+2$$

That means that $q(x) = x^3-3x+2$ divides $x^6+8x^5+2x^4-36x^3+x^2+52x-28$. Since $q(1) = 0$, $(x-1) \mid q(x)$ and $q(x)$ is not irreducible. We have

$$\frac{x^6+8x^5+2x^4-36x^3+x^2+52x-28}{x^3-3x+2} = x^3+8x^2+5x-14$$

Hence

$$x^6+8x^5+2x^4-36x^3+x^2+52x-28 = (x^3-3x+2)(x^3+8x^2+5x-14)$$

We can further factorize x^3-3x+2 and $x^3+8x^2+5x-14$ using this rule or Ruffini's Rule, and in the end we get

$$x^6+8x^5+2x^4-36x^3+x^2+52x-28 = (x-1)^3(x+2)^2(x+7)$$

Note that using the GCD and derivative rule on $x^3+8x^2+5x-14$ is useless, since it is squarefree by Proposition 24.

5 Number of real roots for a polynomial

Proposition 27 (Sturm Algorithm)**.** *Let $f(x) \in \mathbb{R}[x]$. We apply the following modifications to Euclid's Algorithm in the computations of* $\gcd(f(x), f'(x))$

- *We plug back into the computaions not the remainder but the remainder with changed sign*
- *We don't take out negative numeric factors, but only positive ones*

The remainder sequence is $f(x), f'(x), r_1(x), \ldots, r_n(x)$. We use the convention that the sign of a polynomial is the sign of the coefficient of its largest degree term. Then let

- *p is number of sign variation in the sequence $f(x), f'(x), r_1(x), \ldots, r_n(x)$.*
- *q is number of sign variation in the sequence $f(x), f'(x), r_1(x), \ldots, r_n(x)$* changing the sign of the polynomials with odd degree*.*

Then the number of real roots of $f(x)$ is $q - p$.

Remark 28. *When we compute the number of sign variations in a sequence, we skip a* 0 *as non-existent. For example*

- *the number of sign variations of* $[+ + 0 + +]$ *is* 0*;*
- *the number of sign variations of* $[+ + 0 - +]$ *is* 2*;*

The examples are computed using the CoCoA procedure `GCDPolySTURMVerbose`.

Example 29. *We want to know the number of real roots of the polynomial* $x^3 + x^2 + x + 1$.

```
GCDSTURM(x^3+x^2+x+1,3x^2 + 2x + 1)=
(x^3 + x^2 + x + 1)=(1/3x + 1/9)*(3x^2 + 2x + 1)+(4/9x + 8/9)
We divide x^3+x^2+x+1 by 3x^2 + 2x + 1, remainder is 4/9x + 8/9=4/9(x+2)
We take out 4/9 and change sign to the remainder

=GCDSTURM(3x^2 + 2x + 1,-x - 2)=
(3x^2 + 2x + 1)=(-3x + 4)*(-x - 2)+(9)
We divide x^2 + 2x + 1 by -x - 2, remainder is 9=9*1
We take out 9 and change sign to the remainder

=GCDSTURM(-x - 2,-1)=1

The GCD is 1
The remainder sequence is = x^3 + x^2 + x + 1,
                           3x^2 + 2x + 1,
                           -x - 2,
                           -1
p= # sign change of + + - -   =1
q= # sign change of - + + -   =2
   we changed the sign of x^3+... from + to - because its degree is 3, odd
   we changed the sign of -x-2 from - to + because its degree is 1, odd
Number of real roots 2-1=1
```

Example 30. *We want to know the number of real roots of the polynomial* $x^4 - 10x^3 + 10$.

```
GCDSTURM(x^4-10x^3+10,2x^3 - 15x^2)=
(x^4 - 10x^3 + 10)=(1/2x - 5/4)*(2x^3 - 15x^2)+(-75/4x^2 + 10)
We divide x^4 - 10x^3 + 10 by 2x^3 - 15x^2, remainder is -75/4x^2 + 10=5/4(-15x^2 + 8)
We take out 5/4 and change sign to the remainder

=GCDSTURM(2x^3 - 15x^2,15x^2 - 8)=
(2x^3 - 15x^2)=(2/15x - 1)*(15x^2 - 8)+(16/15x - 8)
We divide 2x^3 - 15x^2 by 15x^2 - 8, remainder is 16/15x - 8=8/15(2x - 15)
We take out 8/15 and change sign to the remainder

=GCDSTURM(15x^2 - 8,-2x + 15)=
(15x^2 - 8)=(-15/2x - 225/4)*(-2x + 15)+(3343/4)
We divide 15x^2 - 8 by -2x + 15, remainder is 3343/4 =3343/4*1
We take out 3343/4 and change sign to the remainder

=GCDSTURM(-2x + 15,-1)=1

The GCD is 1

The remainder sequence is = x^4 - 10x^3 + 10,
                            4x^3 - 30x^2,
                            15x^2 - 8,
                            -2x + 15,
                            -1
p= # sign change of + + + - -   =1
q= # sign change of + - + - -   =3
   we changed the sign of 4x^3+... from + to - because its degree is 3, odd
   we changed the sign of -2x+15 from - to + because its degree is 1, odd
Number of real roots 3-1=2
```

Example 31. *We want to know the number of real roots of the polynomial* $3x^4+10x^3+13x^2+8x+2$.

```
GCDSTURM(3x^4 + 10x^3 + 13x^2 + 8x + 2,6x^3 + 15x^2 + 13x + 4)=
(3x^4 + 10x^3 + 13x^2 + 8x + 2)=(1/2x + 5/12)*(6x^3 + 15x^2 + 13x + 4)+(1/4x^2 + 7/12x + 1/3)
We divide 3x^4 + 10x^3 + 13x^2 + 8x + 2 by 6x^3 + 15x^2 + 13x + 4,
remainder is 1/4x^2 + 7/12x + 1/3=1/12(3x^2 + 7x + 4)
We take out 1/12 and change sign to the remainder

=GCDSTURM(6x^3 + 15x^2 + 13x + 4,-3x^2 - 7x - 4)=
(6x^3 + 15x^2 + 13x + 4)=(-2x - 1/3)*(-3x^2 - 7x - 4)+(8/3x + 8/3)
We divide 6x^3 + 15x^2 + 13x + 4 by -3x^2 - 7x - 4, remainder is 8/3x + 8/3=8/3(x+1)
We take out 8/3 and change sign to the remainder
```

```
=GCDSTURM(-3x^2 - 7x - 4,-x-1)=
(-3x^2 - 7x - 4)=(3x + 4)*(-x - 1)+(0)
We divide -3x^2 - 7x - 4 by -x-1, remainder is 0


=GCDSTURM(-x-1,0)=-x-1

The GCD is x+1 (we can change the sign at will, just NOT in the sequence)

The remainder sequence is = 3x^4 + 10x^3 + 13x^2 + 8x + 2,
                            12x^3 + 30x^2 + 26x + 8,
                            -3x^2 - 7x - 4,
                            -x - 1
p= # sign change of + + - -   =1
q= # sign change of + - - +   =2
   we changed the sign of 12x^3+... from + to - because its degree is 3, odd
   we changed the sign of -x-1 from - to + because its degree is 1, odd
Number of real roots 2-1=1
```

6 Homework

We want to know the number of real roots of

1. $p_1(x) = x^3 + x + 3$ [Answer:1]
2. $p_2(x) = 2x^3 - x^2 - 2$ [Answer:1]
3. $p_3(x) = x^4 - x - 2$ [Answer:2]
4. $p_4(x) = x^4 - x^3 - 1$ [Answer:2]
5. $p_5(x) = x^5 - x - 1$ [Answer:1]
6. $p_6(x) = x^{16} - 1$ [Answer:2]
7. $p_6(x) = x^{17} - 1$ [Answer:1]

Solve at least three exercises and send your solutions, with all the computations step by step, by email to `massimo.caboara@unipi.it` *WITH FCS IN THE MESSAGE SUBJECT*, and *NO LATER THAN TUESDAY EVENING*

7 Some exercises

Compute the following GCD's with the minimum of computations:

1. $\gcd(x^9 + x^7 - x, x^2 - 1)$ [Solution 1]

2. $\gcd(x^8 - 1, x^{16} - 1)$ [Solution $x^8 - 1$]

Compute the following derivatives:

1. $((x^4 - 2)(x^2 - 1))'$ [Solution $6x^5 - 4x^3 - 4x$]
2. $((x^4 + 3x - 2)(x^2 + x + 1))'$ [Solution $6x^5 + 5x^4 + 4x^3 + 9x^2 + 2x + 1$]
3. $((x^3 - 1)^2)' =$[Solution $6x^5 - 6x^2$]
4. $((3x^5 - x^2)^3)' =$[Solution $405x^{14} - 324x^{11} + 81x^8 - 6x^5$]

Find the real roots of the following polynomials:

1. $x^7 + 6x^5 - 2x^4 + 9x^3 - 12x^2 - 18$ [Solution $x = \sqrt[3]{2}$]
2. $x^7 - 4x^5 - 5x^4 + 4x^3 + 20x^2 - 20$ [Solution $x = \pm\sqrt{2}, \sqrt[3]{5}$]