XGCD

Into & Live Coding

Euclidean Algorithm

GCD <- Greatest Common Denominator

GCD(a, b) = GCD(b, a % b)

This is useful on itself to get the actual GCD.

Extended Euclidean Algorithm

In addition to the GCD, XGCD provides values s

and t such that:

$GCD(a, b) = as + bt = d$

Extended Euclidean Algorithm

GCD(a, b) = as + bt = d

Why dat useful tho?

If a and b are coprime (the only positive integer that divides both of them is 1) then **s** is the **multiplicative inverse** of **b mod a**.

$x = b^{-1} \bmod a$

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98					
2							
3							
4							
5							
6							

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2							
3							
4							
5							
6							

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44					
3							
4							
5							
6							

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44	2	10			
3							
4							
5							
6							

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44	2	10			
3	44	10					
4							
5							
6							

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44	2	10			
3	44	10	4	4			
4							
5							
6							

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44	2	10			
3	44	10	4	4			
4	10	4					
5							
6							

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44	2	10			
3	44	10	4	4			
4	10	4	2	2			
5							
6							

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44	2	10			
3	44	10	4	4			
4	10	4	2	2			
5	4	2					
6							

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44	2	10			
3	44	10	4	4			
4	10	4	2	2			
5	4	2	2	0			
6							

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44	2	10			
3	44	10	4	4			
4	10	4	2	2			
5	4	2	2	0			
6	2	0					

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44	2	10			
3	44	10	4	4			
4	10	4	2	2			
5	4	2	2	0			
6	2	0	NaN	NaN			

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44	2	10			
3	44	10	4	4			
4	10	4	2	2			
5	4	2	2	0			
6	2	0	NaN	NaN	2	1	0

$s = t_{previous\_row}$

$t = s_{previous\_row} – (a/b)*t_{previous\_row}$

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44	2	10			
3	44	10	4	4			
4	10	4	2	2			
5	4	2	2	0	2	0	1
6	2	0	NaN	NaN	2	1	0

$s = t_{previous\_row}$

$t = s_{previous\_row} – (a/b)*t_{previous\_row}$

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44	2	10			
3	44	10	4	4			
4	10	4	2	2	2	1	-2
5	4	2	2	0	2	0	1
6	2	0	NaN	NaN	2	1	0

$s = t_{previous\_row}$

$t = s_{previous\_row} – (a/b)*t_{previous\_row}$

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44	2	10			
3	44	10	4	4	2	-2	9
4	10	4	2	2	2	1	-2
5	4	2	2	0	2	0	1
6	2	0	NaN	NaN	2	1	0

$s = t_{previous\_row}$

$t = s_{previous\_row} – (a/b)*t_{previous\_row}$

Extended Euclidean Algorithm

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44			
2	98	44	2	10	2	9	-20
3	44	10	4	4	2	-2	9
4	10	4	2	2	2	1	-2
5	4	2	2	0	2	0	1
6	2	0	NaN	NaN	2	1	0

$s = t_{previous\_row}$

$t = s_{previous\_row} – (a/b)*t_{previous\_row}$

Extended Euclidean Algorithm

GCD(240, 98) = (-20)*240 + 49*98 = 2

Row	a	b	a/b	a%b	d	s	t
1	240	98	2	44	2	-20	49
2	98	44	2	10	2	9	-20
3	44	10	4	4	2	-2	9
4	10	4	2	2	2	1	-2
5	4	2	2	0	2	0	1
6	2	0	NaN	NaN	2	1	0

$s = t_{previous\_row}$

$t = s_{previous\_row} - (a/b)*t_{previous\_row}$