EXTENDED EUCLIDEAN ALGORITHM

NUMBER THEORY

Some number theory

- Let *a, b* be integers, then *a* divides *b* if there exists an integer *c* such that *b* = *ac*. In another words, *a* is a divisor of *b*, or *a* is a factor of *b*.
  - E.g., $10 = 2 \times 5$

- If *a* divides *b*, then this is denoted by *a*|*b*.
  - E.g., $2 \mid 10$

Some number theory

- An integer c is *common divisor* of a and b if $c|a$ and $c|b$.
  - E.g., $2 \mid 12$ and $2 \mid 8$, hence 2 is a common divisor of 12 and 8

Some number theory

- A non-negative integer d is the *greatest common divisor* of integers a and b, denoted $d = gcd(a, b)$, if
  - d is a common divisor of a and b; and
  - whenever $c|a$ and $c|b$, then $c|d$.

- Equivalently, $gcd(a,b)$ is the largest positive integer that divides both a and b

- Example 4 = gcd(8, 12)

Some number theory

- Two integers *a* and *b* are said to *be relatively prime* or *coprime* if *gcd(a,b) = 1*.

E.g., 3 and 7 are coprime; that is, gcd(3,7) = 1 because $1 \mid 3$ and $1 \mid 7$. There is no other common divisor that divides both 3 and 7.

Similarly, 3 and 4 are coprime; that is, gcd(3,4) = 1 because $1 \mid 3$ and $1 \mid 4$, and there is no other common divisor that divides both 3 and 4.

Euclidean algorithm

- Euclidean algorithm for computing the greatest common divisor (gcd) of two integers:

INPUT: two non-negative integers a and b with a ≥ b.
OUTUT: the greatest common divisor of a and b.

While b ≠ 0 do the following:
Set r ← a mod b,
a ←b,
b ← r.
Return (a)

Euclidean algorithm

While b ≠ 0 do the following:
Set r ← a mod b,
a ← b,
b ← r.
Return (a)

a b → ?

- Example: gcd(4864, 3458) = 38

a	b	q $= \mathrm{int}(\frac{a}{b})$	r
4864	3458	1	1406
3458	**1406**	**2**	**646**
1406	**646**	**2**	**114**
646	**114**	**5**	**76**
114	**76**	**1**	**38**
76	**38**	**2**	**0**
38	**0**		

If gcd(a, b) = 1,

a, b is co-prime
relatively prime
to each other

Extended euclidean algorithm

$\underline{a^{-1} \bmod b}$

The Euclidean algorithm can be extended so that it not only yields the *greatest common divisor d* of two integers *a* and *b*, but also integers *x* and *y* satisfying *ax* + *by* = *d*; where d = gcd(a,b). In other words,

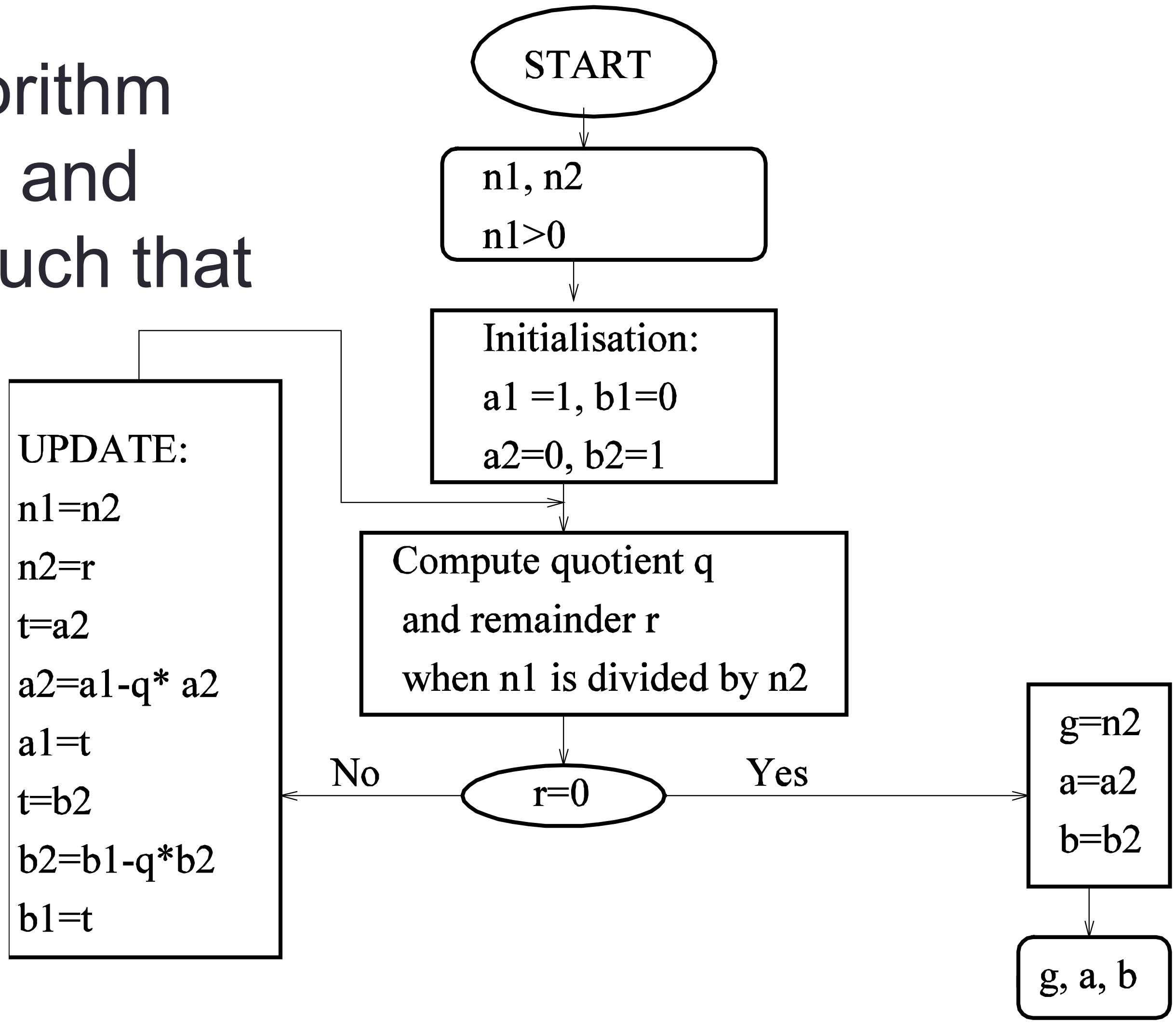
gcd(a,b) = ax + by = d

If *gcd(a,b)* = *1*, then *ax* + *by* = *1*. In such a case,

- *x* is known as $\boxed{a^{-1}}$ *mod b* (multiplicative inverse modulo b), and
- *y* is known as $\boxed{b^{-1}}$ *mod a* (multiplicative inverse modulo a)

Extended euclidean algorithm

- The Extended Euclidean algorithm calculates a, b and $g=\gcd(n_1,n_2)$ such that $g=a*n_1+b*n_2$.



Extended euclidean algorithm

n_1 n_2

Find gcd(4864,3458) and a, b such that

$$4864a + 3458b = \gcd(4864,3458)$$

$\Rightarrow$

Extended euclidean algorithm

init para

n1	n2	r	q	a1	b1	a2	b2
4864	3458			1	0	0	1

Extended euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1

Extended euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1
3458	1406			0	1		

n1 = n2, n2 = r

a1 = a2, b1 = b2

Extended euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1
3458	1406	646	2	0	1	1	-1

$$a2 = a1 - q * a2$$

$$b2 = b1 - q * b2$$

Extended euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1
3458	1406	646	2	0	1	1	-1
1406	646			1	-1		

n1 = n2, n2 = r

a1 = a2, b1 = b2

Extended euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1
3458	1406	646	2	0	1	1	-1
1406	646	114	2	1	-1	-2	3

a2 = a1 – q * a2

b2 = b1 – q * b2

Extended euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1
3458	1406	646	2	0	1	1	-1
1406	646	114	2	1	-1	-2	3
646	114	76	5	-2	3	5	-7

Extended euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1
3458	1406	646	2	0	1	1	-1
1406	646	114	2	1	-1	-2	3
646	114	76	5	-2	3	5	-7
114	76	38	1	5	-7	-27	38

Extended euclidean algorithm

n1	n2	r	q	a1	b1	a2	b2
4864	3458	1406	1	1	0	0	1
3458	1406	646	2	0	1	1	-1
1406	646	114	2	1	-1	-2	3
646	114	76	5	-2	3	5	-7
114	76	38	1	5	-7	-27	38
76	38	0	2	-27	38	32	-45

$$\gcd(4864, 3458) = 38, \textit{ thus } 4864 \times \underset{a}{32} + 3458 \times -45 = 38$$

Extended euclidean algorithm

Find 121^{-1} mod 654

$n2^{-1}$

n1	n2	r	q	a1	b1	a2	b2
654	121			1	0	0	1

Extended euclidean algorithm

Find 121^{-1} mod 654

n1	n2	r	q	a1	b1	a2	b2
654	121	49	5	1	0	0	1

Extended euclidean algorithm

Find $121^{-1} \bmod 654$

n1	n2	r	q	a1	b1	a2	b2
654	121	49	5	1	0	0	1
121	49	23	2	0	1	1	-5

Extended euclidean algorithm

Find 121^{-1} mod 654

n1	n2	r	q	a1	b1	a2	b2
654	121	49	5	1	0	0	1
121	49	23	2	0	1	1	-5
49	23	3	2	1	-5	-2	11

Extended euclidean algorithm

Find $121^{-1} \bmod 654$

n1	n2	r	q	a1	b1	a2	b2
654	121	49	5	1	0	0	1
121	49	23	2	0	1	1	-5
49	23	3	2	1	-5	-2	11
23	3	2	7	-2	11	5	-27

Extended euclidean algorithm

Find $121^{-1} \bmod 654$

n1	n2	r	q	a1	b1	a2	b2
654	121	49	5	1	0	0	1
121	49	23	2	0	1	1	-5
49	23	3	2	1	-5	-2	11
23	3	2	7	-2	11	5	-27
3	2	1	1	5	-27	-37	200

Extended euclidean algorithm

Find $121^{-1} \bmod 654$

n1	n2	r	q	a1	b1	a2	b2
654	121	49	5	1	0	0	1
121	49	23	2	0	1	1	-5
49	23	3	2	1	-5	-2	11
23	3	2	7	-2	11	5	-27
3	2	1	1	5	-27	-37	200
2	1	0	2	-37	200	42	-227

gcd

Extended euclidean algorithm

$$\text{Thus } n1 \times a2 \ + \ n2 \times b2 \ = \ \gcd(n1, n2)$$

$$654 \times 42 \ + \ 121 \times \text{-}227 = 1$$

$$1 = 1$$

Extended euclidean algorithm

Since $\gcd(654,121)=1$, there exist multiplicative inverse:

$a2 =$ multiplicative inverse n1 mod n2, and
$b2 =$ multiplicative inverse n2 mod n1

$$n1 \times a2 \; + \; n2 \times b2 \; = \; \gcd(n1,n2)$$
$$654 \times 42 \; + \; 121 \times -227 = 1$$

$654+(-227)$ $121^{-1} \bmod 654$

$$Thus\ 121^{-1} \bmod 654 = -227 \bmod 654 = \underline{427} \bmod 654$$

$$Check: 427 \times 121 \bmod 654 \overset{?}{=} 1 \bmod 654$$

Extended euclidean algorithm

Find the multiplicative inverse of 1234 mod 4321.

n1	n2	r	q	a1	b1	a2	b2
4321	1234			1	0	0	1

Extended euclidean algorithm

Find the multiplicative inverse of 1234 mod 4321.

n1	n2	r	q	a1	b1	a2	b2
4321	1234	619	3	1	0	0	1

Extended euclidean algorithm

Find the multiplicative inverse of 1234 mod 4321.

n1	n2	r	q	a1	b1	a2	b2
4321	1234	619	3	1	0	0	1
1234	619	615	1	0	1	1	-3

Extended euclidean algorithm

Find the multiplicative inverse of 1234 mod 4321.

n1	n2	r	q	a1	b1	a2	b2
4321	1234	619	3	1	0	0	1
1234	619	615	1	0	1	1	-3
619	615	4	1	1	-3	-1	4

Extended euclidean algorithm

Find the multiplicative inverse of 1234 mod 4321.

n1	n2	r	q	a1	b1	a2	b2
4321	1234	619	3	1	0	0	1
1234	619	615	1	0	1	1	-3
619	615	4	1	1	-3	-1	4
615	4	3	153	-1	4	2	-7

Extended euclidean algorithm

Find the multiplicative inverse of 1234 mod 4321.

n1	n2	r	q	a1	b1	a2	b2
4321	1234	619	3	1	0	0	1
1234	619	615	1	0	1	1	-3
619	615	4	1	1	-3	-1	4
615	4	3	153	-1	4	2	-7
4	3	1	1	2	-7	-307	1075

Extended euclidean algorithm

Find the multiplicative inverse of 1234 mod 4321.

n1	n2	r	q	a1	b1	a2	b2
4321	1234	619	3	1	0	0	1
1234	619	615	1	0	1	1	-3
619	615	4	1	1	-3	-1	4
615	4	3	153	-1	4	2	-7
4	3	1	1	2	-7	-307	1075
3	1	0	3	-307	1075	309	-1082

GCD

Extended euclidean algorithm

From the above, we have:

$$4321 \times \underline{309} + 1234 \times -\underline{1082} = 1$$

Thus

$$x = 309 \mod 1234, \textit{ and}$$
$$y = -1082 \mod 4321 = 3239 \mod 4321$$

$1234^{-1} \bmod 4321 = 3239$

Check:

$$309 \times 4321 \mod 1234 = 1 \mod 1234$$
$$3239 \times 1234 \mod 4321 = 1 \mod 4321$$