Some fundamental properties of gcds

Lemma 62 *For all positive integers* l, m, *and* n,

1. ***(Commutativity)*** $\gcd(m, n) = \gcd(n, m)$,
2. ***(Associativity)*** $\gcd\big(l, \gcd(m, n)\big) = \gcd(\gcd(l, m), n)$,
3. ***(Linearity)***[a] $\gcd(l \cdot m, l \cdot n) = l \cdot \gcd(m, n)$.

PROOF:

[a] Aka (Distributivity).

given m, n. $\Rightarrow$ $\ell n | \ell m$.

$\ell m = q(\ell n) + \ell r$
$0 \le \ell r < \ell n$

- $\gcd(m,n)$
  - $n|m$: n
  - $m \geq n$, $m = q \cdot n + r$, $0 \le r < n$: $\gcd(n,r)$
    - r
    - $\vdots$
    - $\gcd(a,b)$
      - b
      - $\vdots$
  - $n > m$: $\gcd(n,m)$
    - m

- $\gcd(\ell m, \ell n)$
  - $\ell \cdot n$
  - $\ell m \geq \ell n$: $\gcd(\ell n, \ell r)$
    - ℓr
    - $\vdots$
    - $\gcd(\ell a, \ell b)$
      - ℓb
      - $\vdots$
  - $\ell n > \ell m$: $\gcd(\ell n, \ell m)$
    - ℓm

output
$\gcd(m,n)$

$$\boxed{\ell \cdot \gcd(m,n) = \gcd(\ell m, \ell n)}$$

Euclid's Theorem

Theorem 63 *For positive integers* k, m, *and* n, *if* $k \mid (m \cdot n)$ *and* $\gcd(k, m) = 1$ *then* $k \mid n$.

PROOF: Consider integers k, m, n.

Assume: ① $k \mid (m.n)$ and ② $\gcd(k, m) = 1$

From ②, $n . \gcd(k, m) = n$

// by linearity

$\gcd(nk, mn)$

// by ①

$\gcd(nk, \ell k)$ for some int ℓ

// by linearity

$k . \gcd(n, \ell)$

$\Longrightarrow$ $k \mid n$ $\boxtimes$

Corollary 64 (Euclid's Theorem) *For positive integers m and n, and prime p, if $p \mid (m \cdot n)$ then $p \mid m$ or $p \mid n$.*

Now, the second part of Fermat's Little Theorem follows as a corollary of the first part and Euclid's Theorem.

PROOF: Let m, n be pos. int. Let p be a prime

Assume $p \mid (m.n)$

RTP: $p \mid m \vee p \mid n$

We argue by cases:

1. If $p \mid m$ then we are done.
2. If $\neg(p \mid m)$ then $\gcd(p,m)=1$ and by the previous thm $p \mid n$.

$\boxtimes$

Recall

For p prime $\quad p \mid \binom{p}{m} \quad 0 < m < p$

$$\binom{p}{m} = p\,\frac{(p-1)!}{m!\,(p-m!)}$$

$$\Rightarrow \left[m!\,(p-m)!\right]\cdot\binom{p}{m} = p\cdot(p-1)!$$

$$\Rightarrow p \mid \left[m!\,(p-m)!\right]\cdot\binom{p}{m} \wedge p \nmid \left[m!\cdot(p-m)!\right]$$

$$\Rightarrow p \mid \binom{p}{m}.$$

FLT : $i^p \equiv i \pmod p$

$i \not\equiv 0 \pmod p$

?

$i^{p-1} \equiv 1 \pmod p$ $\quad$ i not a multiple of p

Fields of modular arithmetic

Corollary 66 *For prime* p*, every non-zero element* i *of* $\mathbb{Z}_p$ *has* $[i^{p-2}]_p$ *as multiplicative inverse. Hence,* $\mathbb{Z}_p$ *is what in the mathematical jargon is referred to as a* field.

$i^p \equiv i \pmod p \Rightarrow p \mid (i^p - i) = (i^{p-1} - 1) \cdot i$

If $p \nmid i$ then $p \mid i^{p-1} - 1 \Leftrightarrow i^{p-1} \equiv 1 \pmod p$.

Extended Euclid's Algorithm

Example 67

quotients remainders.

$$
\begin{array}{rl|lcrcrcl}
 & \gcd(34,13) & 34 & = & 2\cdot & 13 & + & 8 \\
= & \gcd(13,8) & 13 & = & 1\cdot & 8 & + & 5 \\
= & \gcd(8,5) & 8 & = & 1\cdot & 5 & + & 3 \\
= & \gcd(5,3) & 5 & = & 1\cdot & 3 & + & 2 \\
= & \gcd(3,2) & 3 & = & 1\cdot & 2 & + & 1 \\
= & \gcd(2,1) & 2 & = & 2\cdot & 1 & + & 0 \\
= & 1 & & & & & &
\end{array}
$$

Extended Euclid's Algorithm

Example 67

remainders

$$
\begin{array}{rl||rcrcrcr||rcrcrcr}
 & \gcd(34,13) & 34 & = & 2\cdot & 13 & + & 8 & 8 & = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 13 & = & 1\cdot & 8 & + & 5 & 5 & = & 13 & -1\cdot & 8 \\
= & \gcd(8,5) & 8 & = & 1\cdot & 5 & + & 3 & 3 & = & 8 & -1\cdot & 5 \\
= & \gcd(5,3) & 5 & = & 1\cdot & 3 & + & 2 & 2 & = & 5 & -1\cdot & 3 \\
= & \gcd(3,2) & 3 & = & 1\cdot & 2 & + & 1 & 1 & = & 3 & -1\cdot & 2 \\
= & \gcd(2,1) & 2 & = & 2\cdot & 1 & + & 0 & & & & & \\
= & 1 & & & & & & & & & & &
\end{array}
$$

integer linear combination

$$
\begin{array}{rl||rcrrr}
 & \gcd(34,13) & 8 & = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 & = & 13 & -1\cdot & 8 \\
= & \gcd(8,5) & 3 & = & 8 & -1\cdot & 5 \\
= & \gcd(5,3) & 2 & = & 5 & -1\cdot & 3 \\
= & \gcd(3,2) & 1 & = & 3 & -1\cdot & 2
\end{array}
$$

$$
\begin{array}{rl||rcccc}
 & \gcd(34,13) & 8 = & & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & & 13 & -1\cdot & 8 \\
 & & = & & 13 & -1\cdot & \overbrace{(34-2\cdot 13)} \\
 & & = & -1\cdot 34 + 3\cdot 13 & & & \\
= & \gcd(8,5) & 3 = & & 8 & -1\cdot & 5 \\
 & & & & & & \\
= & \gcd(5,3) & 2 = & & 5 & -1\cdot & 3 \\
 & & & & & & \\
= & \gcd(3,2) & 1 = & & 3 & -1\cdot & 2
\end{array}
$$

$$
\begin{array}{rl||rccc}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)} \\
 & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
 & & = & \overbrace{(34-2\cdot 13)} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)} \\
 & & = & 2\cdot 34+(-5)\cdot 13 & & \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
 & & & & & \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2
\end{array}
$$

$$
\begin{array}{rl||rcccc}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)} \\
 & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
 & & = & \overbrace{(34-2\cdot 13)} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)} \\
 & & = & 2\cdot 34+(-5)\cdot 13 & & \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
 & & = & \overbrace{-1\cdot 34+3\cdot 13} & -1\cdot & \overbrace{(2\cdot 34+(-5)\cdot 13)} \\
 & & = & -3\cdot 34+8\cdot 13 & & \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2
\end{array}
$$

Fact: gcd(m,n) is an integer linear combination of m and n.

$$
\begin{array}{rl|rlcc}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)}^{8} \\
 & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
 & & = & \overbrace{(34-2\cdot 13)}^{8} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)}^{5} \\
 & & = & 2\cdot 34+(-5)\cdot 13 & & \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
 & & = & \overbrace{-1\cdot 34+3\cdot 13}^{5} & -1\cdot & \overbrace{(2\cdot 34+(-5)\cdot 13)}^{3} \\
 & & = & -3\cdot 34+8\cdot 13 & & \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2 \\
 & & = & \overbrace{(2\cdot 34+(-5)\cdot 13)}^{3} & -1\cdot & \overbrace{(-3\cdot 34+8\cdot 13)}^{2} \\
 & & = & 5\cdot 34+(-13)\cdot 13 & &
\end{array}
$$

coefficients

Linear combinations

Definition 68 *An integer* r *is said to be a* [linear combination]() *of a pair of integers* m *and* n *whenever*

> *there exist a pair of integers* s *and* t*, referred to as the* coefficients *of the linear combination, such that*
>
> $$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \ ;$$
>
> *that is*
>
> $$s \cdot m + t \cdot n = r \ .$$

NB: Coefficients are not unique

Suppose $\gcd(m,n)=1$ [m and n are coprime]

$\Rightarrow$ $s\cdot m + t\cdot n = 1$ with s and t efficiently computed

$\Rightarrow$ $t\cdot n \equiv 1 \pmod{m}$ and so t is a multiplicative inverse of n in $\mathbb{Z}_m$.

Theorem 69 *For all positive integers* m *and* n,

1. $\gcd(m, n)$ *is a linear combination of* m *and* n, *and*
2. *a pair* $lc_1(m, n)$, $lc_2(m, n)$ *of integer coefficients for it, i.e. such that*

$$\begin{bmatrix} lc_1(m,n) & lc_2(m,n) \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = \gcd(m,n) \quad ,$$

can be efficiently computed.

Proposition 70 *For all integers m and n,*

1. $\begin{bmatrix} \overset{1}{?_1} & \overset{0}{?_2} \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \quad \wedge \quad \begin{bmatrix} \overset{0}{?_1} & \overset{1}{?_2} \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$;

Proposition 70 *For all integers* m *and* n*,*

1. $\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \quad \wedge \quad \begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$ *;*

2. *for all integers* s_1, t_1, r_1 *and* s_2, t_2, r_2,

$$\begin{bmatrix} s_1 & t_1 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 \quad \wedge \quad \begin{bmatrix} s_2 & t_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_2$$

implies s_1+s_2 t_1+t_2

$$\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2 \; ;$$

Proposition 70 *For all integers* m *and* n,

1. $\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \;\wedge\; \begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$;

2. *for all integers* s_1, t_1, r_1 *and* s_2, t_2, r_2,

   $$\begin{bmatrix} s_1 & t_1 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 \;\wedge\; \begin{bmatrix} s_2 & t_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_2$$

   implies

   $$\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2 \;;$$

3. *for all integers* k *and* s, t, r,

   $$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \text{ implies } \begin{bmatrix} \overset{k\cdot s}{?_1} & \overset{k\cdot t}{?_2} \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = k \cdot r \;.$$

gcd

```
fun  gcd( m , n )
= let
    fun  gcditer( [s1, t1] r1  ,  c as [s2, t2] r2  )
    = let
        val (q,r) = divalg(r1,r2)   (* r = r1-q*r2 *)
      in
        if r = 0
        then  c
        else  gcditer(  c ,  [s1-q*s2  t1-q*t2] r  )
      end
  in
    gcditer( [1 0] m  ,  [0 1] n  )
  end
```

egcd

```
fun egcd( m , n )
= let
    fun egcditer( ((s1,t1),r1) , lc as ((s2,t2),r2) )
    = let
        val (q,r) = divalg(r1,r2)    (* r = r1-q*r2 *)
      in
        if r = 0
        then lc
        else egcditer( lc , ((s1-q*s2,t1-q*t2),r) )
      end
  in
    egcditer( ((1,0),m) , ((0,1),n) )
  end
```

```
fun gcd( m , n ) = #2( egcd( m , n ) )

fun lc1( m , n ) = #1( #1( egcd( m , n ) ) )

fun lc2( m , n ) = #2( #1( egcd( m , n ) ) )
```

Multiplicative inverses in modular arithmetic

Corollary 74 *For all positive integers* m *and* n*,*

1. $n \cdot \mathrm{lc}_2(m, n) \equiv \gcd(m, n) \pmod{m}$*, and*
2. *whenever* $\gcd(m, n) = 1$*,*

   $\big[\mathrm{lc}_2(m, n)\big]_m$ *is the multiplicative inverse of* $[n]_m$ *in* $\mathbb{Z}_m$ *.*