Properties of GCDs and Applications

PROOF PRINCIPLE

To prove that a natural number k is the greatest common divisor of two natural numbers m and n show that

(i) $k \mid m \wedge k \mid n$

(ii) for all natural numbers d,

$$(d \mid m \wedge d \mid n) \Rightarrow d \mid k$$

Proposition For all natural numbers m and n,

$$\gcd(m,n) = m \iff m \mid n.$$

PROOF: Let m and n be natural numbers.

($\Rightarrow$) Assume $\gcd(m,n)=m$.

<u>RTP</u> $m \mid n$

Know that $\gcd(m,n) \mid n$.

($\Leftarrow$) Assume $m \mid n$.

<u>RTP</u>: $\gcd(m,n) \stackrel{?}{=} m$

equivalently

RTP: (i) $m \mid m \wedge m \mid n$

(ii) for all nat. numbers d

$$(d \mid m \wedge d \mid n) \Rightarrow d \mid m$$

$\boxtimes$

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).

PROOF: Let m, n, ℓ be positive integers.

RTP: $\gcd(\ell m, \ell n) = \ell \cdot \gcd(m,n)$

We use the proof principle and show

(i) $\ell \cdot \gcd(m,n) \mid \ell m$

$\wedge\ \ell \cdot \gcd(m,n) \mid \ell n$

(ii) for all natural numbers d,

$(d \mid \ell m \wedge d \mid \ell n) \Rightarrow d \mid \ell \cdot \gcd(m,n)$

(i) <u>RTP</u> $\quad l \cdot \gcd(m,n) \mid lm$

Since $\gcd(m,n) \mid m$, it follows that

$l \cdot \gcd(m,n) \mid l \cdot m$.

<u>RTP</u> $\quad l \cdot \gcd(m,n) \mid ln$

Since $\gcd(m,n) \mid n$, we have that

$l \cdot \gcd(m,n) \mid l \cdot n$.

(ii) Let d be a natural number such that

① $d \mid \ell m$ and ② $d \mid \ell n$.

RTP $d \mid \ell \cdot \gcd(m,n)$

Lemma $\gcd(\ell m, \ell n) \mid \ell \cdot \gcd(m,n)$

PROOF: Note that $\ell \mid \ell m$ and $\ell \mid \ell n$.

Therefore $\ell \mid \gcd(\ell m, \ell n)$; that is,

$\gcd(\ell m, \ell n) = \ell k$ for some integer k.

It follows $\ell k \mid \ell m$ and $\ell k \mid \ell n$.

By cancellation, $k \mid m$ and $k \mid n$. Thus

$k \mid \gcd(m,n)$ and so $\ell k \mid \ell \cdot \gcd(m,n)$. $\boxtimes$

(ii) Let d be a natural number such that

① $d \mid lm$ and ② $d \mid ln$.

RTP $d \mid l \cdot \gcd(m,n)$

Lemma $\gcd(lm, ln) \mid l \cdot \gcd(m,n)$

Assume ① and ②. Then $d \mid \gcd(lm, ln)$ and as $\gcd(lm, ln) \mid l \cdot \gcd(m,n)$ it follows that $d \mid l \cdot \gcd(m,n)$.

$\boxtimes$

COPRIMALITY

Definition Two natural numbers are said to be coprime whenever their greatest common divisor is 1.

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: Let k, m, n be positive integers.

Assume: ① $k \mid (m \cdot n)$; ie, $m \cdot n = k\ell$ for some int ℓ

② $\gcd(k, m) = 1$

RTP $k \mid n$.

By ②, $n = n \cdot \gcd(k, m) = \gcd(n \cdot k, n \cdot m)$

$= \gcd(nk, k \cdot \ell) = k \cdot \gcd(n, \ell)$

Therefore $k \mid n$. $\boxtimes$

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

PROOF: Let m and n be positive integers, and let p be a prime.

<u>Assume:</u> $p \mid (m \cdot n)$

<u>RTP</u> $p \mid m$ or $p \mid n$

<u>CASE</u> $p \mid m$ we are done

<u>CASE</u> $p \nmid m$ Then $\gcd(p, m) = 1$ and since $p \mid (m \cdot n)$ we are done by the previous theorem. $\boxtimes$

Recall For all natural numbers i and primes p,

$$i^p \equiv i \pmod{p}$$

Corollary If i is not a multiple of p then

$$i^{p-1} \equiv 1 \pmod{p}$$

PROOF: Let i be a natural number not multiple of a prime p. We have seen $p \mid i^p - i = i(i^{p-1} - 1)$ and $p \nmid i$. Therefore, $p \mid (i^{p-1} - 1)$.

$\boxtimes$

Corollary For all primes p and integers m. If $0<m<p$ then $p \mid \binom{p}{m}$.

PROOF: Let p be a prime and let m be a positive integer below p.

Note that
$$(p-m)\binom{p}{m} = p\cdot\binom{p-1}{m}.$$

Therefore
$$p \mid (p-m)\cdot\binom{p}{m}$$
But p and $p-m$ are coprime. Thus, $p \mid \binom{p}{m}$.

$\boxtimes$

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.*