PROJECTED WRITTEN NOTES FROM THE M325K LECTURE ON TUESDAY, APRIL 2, 2024, on Sec. 8.5: THE EUCLIDEAN ALGORITHM for FINDING the GCD, and SEC. 8.4 (Epp's 4th Edition): Expressing gcd(a,b) as as + tb, Modular Inverses, and Simple Congruences

CLASS #21

---

**Defn**: Let a and b be two positive integers.

A common divisor of a and b is an integer d such that $d|a$ and $d|b$.

Ex: 7 is a common divisor of 21 and 35

The Greatest Common Divisor of a and b, denoted gcd(a,b), is the greatest of all common divisors of a and b.

Ex: gcd(40,24) = 8

The positive common divisors 1, 2, 4, 8

Also: NO common prime factors

$40 = 8 \cdot 5$

$24 = 8 \cdot 3$

---

Ex: gcd(3258, 642) = 6 (as it turns out)

---

Read The Handout "The Euclidean Algorithm for FINDING gcd(a,b)".

# THE EUCLIDEAN ALGORITHM FOR FINDING $\gcd(a,b)$

when $a > b$ and both are $> 0$.

**STEP**

① DIVIDE $b \overline{)\, a}$ with quotient $q_1$, remainder $r_1$ — $a$ = the larger of the two #'s

If $r_1 = 0$, $b \mid a$ and $\gcd(a,b) = b$

② DIVIDE $r_1 \overline{)\, b}$ with quotient $q_2$, remainder $r_2$ — $0 < r_2 < r_1$

⋮ ⋮

(k) DIVIDE $r_{k-1} \overline{)\, r_{k-2}}$ with quotient $q_k$, remainder $r_k$ — $0 < r_k < r_{k-2}$

(k+1) DIVIDE $r_k \overline{)\, r_{k-1}}$ with quotient $q_{k+1}$, remainder $0$ = when Remainder = 0, STOP!

$\gcd(a,b) = r_k$ = The LAST NON-ZERO REMAINDER

# EXAMPLE APPLICATIONS OF THE EUCLIDEAN ALGORITHM:

FIND $\gcd(63, 72)$

$$\begin{array}{r} 1 \\ 63\overline{)72} \\ -63 \\ \hline 9 \end{array} \quad \dashrightarrow \quad \begin{array}{r} 7 \\ 9\overline{)63} \\ -63 \\ \hline 0 \end{array} \quad \text{STOP!}$$

$\gcd(63, 72) = 9$

---

FIND $\gcd(3258, 642)$

$$\begin{array}{r} 5 \\ 642\overline{)3258} \\ -3210 \\ \hline 48 \end{array} \quad \dashrightarrow \quad \begin{array}{r} 13 \\ 48\overline{)642} \\ 48 \\ \hline 162 \\ 144 \\ \hline 18 \end{array} \quad \dashrightarrow \quad \begin{array}{r} 2 \\ 18\overline{)48} \\ -36 \\ \hline 12 \end{array}$$

$$\begin{array}{r} 1 \\ 12\overline{)18} \\ -12 \\ \hline 6 \end{array} \qquad \begin{array}{r} 2 \\ 6\overline{)12} \\ -12 \\ \hline 0 \end{array} \quad \text{STOP!}$$

$\gcd(642, 3258) = 6$

Be sure to read Example 8.5.2 beginning at bottom of page 390 of the EPP BRIEF EDITION TEXTBOOK.

**Def'n:** Two positive non-zero integers, $a$ and $b$ are

**Relatively Prime Integers**

if $\gcd(a,b) = 1$.

This occurs if and only if $a$ and $b$ have no common prime factor.

So, $\gcd(15, 56) = 1$

$3 \cdot 5$, $2^3 \cdot 7$

↖ no common prime factor!

**Defn**: Let $a$ and $b$ and $K$ be integers.

"$K$ is a linear combination of $a$ and $b$"

$\Longleftrightarrow$

There exist integers $s$ and $t$ such that

$$K = as + bt.$$

---

Ex: $K = 53$ is a linear combination of 4 and 7 because

$$53 = 4 \times 8 + 7 \times 3 = 32 + 21 = 53$$

$$K = a \cdot s + b \cdot t$$

---

**FACT**: Given positive integers $a$ and $b$ their gcd, $d = \gcd(a,b)$, is a linear combination of $a$ and $b$; that is,

$d = as + bt$ for some integers $s$ and $t$.

---

Read the Handout

"Expressing $d = \gcd(a,b)$ as $d = as + bt$"

---

**EXAMPLE 1:** Let $a = 330$ and $b = 156$.

EXPRESS $\gcd(330, 156) = 6$ AS A LINEAR COMBINATION OF $a = 330$ and $b = 156$.

I.
$$156 \overline{)330}\ 2 \quad -312 \quad 18$$
$$18 \overline{)156}\ 8 \quad -144 \quad 12$$
$$12 \overline{)18}\ 1 \quad -12 \quad 6$$
$$6 \overline{)12}\ 2 \quad -12 \quad 0$$
GCD = 6

II. $18 = (330)(1) - (156)(2)$

$12 = (156)(1) - (18)(8)$

$6 = (18)(1) - (12)(1)$

III. $6 = (18)(1) - [(156)(1) - (18)(8)](1)$

$6 = (18)(9) - (156)(1)$

$6 = [(330)(1) - (156)(2)](9) - (156)(1)$

$6 = (330)(9) - (156)(+19)$ $\quad [2 \times 9 + 1 = 19]$

$\therefore\ 6 = (330)(9) + (156)(-19)$

EXAMPLE 2: Let $a = 78$ and $b = 23$.

EXPRESS $\gcd(78, 23) = 1$ as a LINEAR COMBINATION OF $a = 78$ and $b = 23$.

I.
$$23\overline{)78}\ 3,\ -69,\ 9 \qquad 9\overline{)23}\ 2,\ -18,\ 5 \qquad 5\overline{)9}\ 1,\ -5,\ 4 \qquad 4\overline{)5}\ 1,\ -4,\ 1 \qquad 1\overline{)4}\ 4,\ -4,\ 0$$

↑ GCD = 1

II. $9 = (78)(1) - (23)(3)$

$5 = (23)(1) - (9)(2)$

$4 = (9)(1) - (5)(1)$

$1 = (5)(1) - (4)(1)$

III. $1 = (5)(1) - [(9)(1) - (5)(1)](1)$

$1 = (5)(2) - (9)(1)$

$1 = [(23)(1) - (9)(2)](2) - (9)(1)$

$1 = (23)(2) - (9)(5)$ $\quad [2 \cdot 2 + 1 = 5]$

$1 = (23)(2) - [(78)(1) - (23)(3)](5)$

$1 = (23)(17) - (78)(5)$ $\quad [2 + 3 \cdot 5 = 17]$

$\therefore\ 1 = (23)(17) + (78)(-5)$

**Defn:** Let $a$ and $b$ and $n$ be integers with $n \geq 1$,

"$a$ is (mod $n$) inverse of $b$"

$\Leftrightarrow$

$ab \equiv 1 \pmod{n} \Leftrightarrow ab = nk + 1$ for some $k \in \mathbb{Z}$, by Theorem 8.4.1.

Ex: Let $n = 7$. We discuss (mod 7) Inverses!

We will show that 23 is a (mod 7) inverse of 32.

[NTS: $(23)(32) \equiv 1 \pmod{7}$]

$(23)(32) = 736 = (7)(105) + 1$.

$736 \equiv 1 \pmod{7}$ by Thm 8.4.1.

$\therefore (23)(32) \equiv 1 \pmod{7}$

$\therefore$ 23 is a (mod 7) inverse of 32.

23 is an inverse (mod 7) of 32.

} BOTH WORDINGS ARE OK.

**Question:** Given positive integers $k$ and $n$,

how can we know if a $(\bmod n)$ inverse of $k$ exist?

And, if such exists, how do we find a number that is a $(\bmod n)$ inverse of $k$?

---

**FACT**: A $(\bmod n)$ inverse of $k$ exists

$\Leftrightarrow$

$\gcd(k, n) = 1$

$\Leftrightarrow$

$k$ and $n$ are relatively prime.

---

Since $\gcd(6, 34) = 2$, a $(\bmod 34)$ inverse of 6 does not exist.

Since $\gcd(78, 23) = 1$,

a $(\bmod 23)$ inverse of 78 exists,

i.e. There exists an integer $l$ such that

$(78)(l) \equiv 1 \pmod{23}$.

---

How do we discover one of these (mod 23) inverses of 78?

Express $1 = \gcd(78, 23)$ as a linear combination of 78 and 23;

Find $s$ and $t$ such that

$$78s + 23t = 1$$

$$(78)(s) = (23)(-t) + 1$$

$$a = n \cdot k + 1$$

$\therefore$ by Theorem 8.4.1,

$$(78)(s) \equiv 1 \pmod{23}$$

$s$ is a (mod 23) inverse of 78.

---

$$1 = (23)(17) + (78)(-5)$$

$$a = n \cdot k + b$$

$\therefore 1 \equiv (78)(-5) \pmod{23}$, by Thm 8.4.1

So, $-5$ is a (mod 23) inverse of 78.

---

FACT: If $s$ is a (mod $n$) inverse of $k$ and $y$ is an integer such that $y \equiv s \pmod{n}$,

Then, $ks \equiv 1 \pmod{n}$ since $s$ is a (mod $n$) inverse of $k$

and

$k \equiv k \pmod{23}$, and $y \equiv s \pmod{23}$

$ky \equiv ks \pmod{23}$ and $ks \equiv 1 \pmod{23}$

So, $ky \equiv 1 \pmod{23}$ by Thm 8.4.3.

So. $y$ is also a (mod $n$) inverse of $k$.

$-5+23 = 18$, so $18 \equiv -5 \pmod{23}$,

So 18 is also a (mod 23) inverse of 78

$(78)(18) \equiv (78)(-5) \pmod{23}$

$(78)(-5) \equiv 1 \pmod{23}$.

$\therefore (78)(18) \equiv 1 \pmod{23}$

by Thm 8.4.3. ✓

## FINDING AN INVERSE OF N (mod n)

GIVEN INTEGERS $N$ and $n$ such that $\gcd(N,n)=1$, an INVERSE OF $N \pmod n$ is an integer $s$ such that $Ns \equiv 1 \pmod n$.

If $\gcd(N,n) \neq 1$, then no such integer $s$ exists!

If $\gcd(N,n)=1$, then such an integer $s$ exists!

Assuming that $\gcd(N,n)=1$,

perform the process to express the gcd (which equals 1 here) as

$$1 = Ns + nt.$$

① The integer $s$ is an INVERSE OF $N \pmod n$

and ② If $x$ is any other integer such that $x \equiv s \pmod n$, then $x$ is also an inverse of $N \pmod n$.

EXAMPLE: Let $N=60$ and $n=7$. FIND AN INVERSE OF $60 \pmod 7$. [Sol'n: $s=2$ is an inverse of $60 \pmod 7$.]

Perform the process to get $1 = (60)(2) + (7)(-17)$

Let $s=2$. $Ns \equiv 1 \pmod 7$:

$(60)(2) \equiv 1 \pmod 7$ since $\left[1-(60)(2)\right] = (7)(-17)$

so $7 \mid \left[1-(60)(2)\right] = (1-Ns)$, so $(60)(2) \equiv 1 \pmod 7$

Def'n: A Simple Congruence is

statement of congruence (mod n) that

involves a variable,

$$Bx \equiv D \pmod{n}$$ such that

$$\gcd(B, n) = 1.$$

Ex: $7x \equiv 2 \pmod{64}$ and $\gcd(7, 64) = 1$,

so $7x \equiv 2 \pmod{64}$ is a Simple

Congruence.

A solution of "$Bx \equiv D \pmod{n}$" is a particular

integer $x_0$ such that

when $x$ is replaced by $x_0$, the

congruence becomes a true statement!

For example: for the congruence "$7x \equiv 2 \pmod{64}$",

$x_0 = 174$ is a solution of it, because

$$(7)(174) = 1288 = (64)(19) + 2$$

$$a = nk + b$$

$$(7)(174) \equiv 2 \pmod{64}$$ by Thm 8.4.1.