Recall,

$$\gcd(a,b) = \max\{d : d|a \text{ and } d|b\}$$

Ex: $\gcd(22, 88)$

$d|22 \Rightarrow d = 1, 2, 11, 22$

$d|88 \Rightarrow d = 1, 2, 4, 8, 11, 22, 44, 88$

GCD Algorithm v.0:

GOAL: To find $\gcd(a,b)$

(1) Apply the fundamental theorem of arith.

(!) This requires factoring which is HARD.

$a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ for $e_i \geq 0$

$b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$ for $f_j \geq 0$

(2) Output $d = p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \cdots p_n^{\min\{e_n, f_n\}}$

Ex: $\gcd(22, 88)$

$= \gcd(2^1 \cdot 11^1, 2^3 \cdot 11^1)$

$= 2^{\min\{1,3\}} 11^{\min\{1,1\}}$

$= 2^1 \cdot 11^1 = 22$

Ex: $\gcd(6, 35)$

$= \gcd(2^1 3^1 5^0 7^0, 2^0 3^0 5^1 7^1)$

$= 2^{\min\{1,0\}} 3^{\min\{1,0\}} \cdot 5^{\min\{0,1\}} \cdot 7^{\min\{0,1\}}$

$= 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^0 = 1$

Lemma: $\gcd(a,b) = \gcd(a, b-a)$

we relate divisors of (a and b) to (a and b-a)

If $d|a$ and $d|b$ then $d|(b-a)$
Thus, $\gcd(a,b) \leq \gcd(a, b-a)$

$S \subseteq T \Rightarrow \max S \leq \max T$

If $d|a$ and $d|(b-a)$ then $d|b$
Thus, $\gcd(a, b-a) \leq \gcd(a,b)$

GCD Algorithm V.1:

GOAL: To find $\gcd(a,b)$

If $a=b$ output a
If $a<b$ output $\gcd(a, b-a)$! Recursion.
If $a>b$ output $\gcd(a-b, a)$

Ex: $\gcd(22, 88)$
$= \gcd(22, 66)$
$= \gcd(22, 44)$
$= \gcd(22, 22)$
$= 22$

Ex: $\gcd(13, 8)$
$= \gcd(5, 8)$
$= \gcd(5, 3)$
$= \gcd(2, 3)$
$= \gcd(2, 1)$
$= \gcd(1, 1)$
$= 1$

"Fun" Fact: If $a \leq b$ and $F_n \leq b \leq F_{n+1}$

Lamé's Thm then it takes at most n steps

COMPUTATIONAL COMPLEXITY to calculate $\gcd(a,b)$

MAT 246 Wk 4a

Recall,

If $d|a$ ad $d|b$ and $b = qa + r$ then $d|r$

GCD Algorithm v.2:

GOAL: To find $\gcd(a,b)$ where $a \leq b$

If $a = 0$ then output b.

If $a = b$ then output a.

If $a < b$ then

$b = qa + r$

and output $\gcd(r, a)$

NB: $\gcd(0,b) = b$ since $b|0$.

Ex: Use the Euclidean Algorithm to compute $\gcd(10, 103)$

$103 = 10 \cdot 10 + 3$ # $\gcd(103, 10)$

$10 = 3 \cdot 3 + 1$ # $\gcd(3, 10)$

$3 = 3 \cdot 1 + 0$ # $\gcd(3, 1)$

Ex: Use the Euclidean algorithm to compute $\gcd(13, 8)$

$13 = 1 \cdot 8 + 5$ # $\gcd(13, 8)$

$8 = 1 \cdot 5 + 3$ # $\gcd(5, 8)$

$5 = 1 \cdot 3 + 2$ # $\gcd(5, 3)$

$3 = 1 \cdot 2 + 1$ # $\gcd(2, 3)$

$2 = 2 \cdot 1 + 0$ # $\gcd(2, 1)$

$\gcd(0, 1)$

Defn: A LINEAR DIOPHANTINE EQUATION has the form $Ax+By=C$ where $A,B,C \in \mathbb{Z}$ and we seek $x,y \in \mathbb{Z}$.

Ex: Use the Euc. Algo. to solve $13x+5y=1$.

\# apply the Euc. Algo.

$13 = 2\cdot 5 + 3$

$5 = 1\cdot 3 + 2$

$3 = 1\cdot 2 + 1$

\# Reverse the steps.

Thus, $1 = 3 - 2$

$= (13-2\cdot 5) - (5-3)$

$= (13-2\cdot 5) - (5-[13-2\cdot 5])$

$= 2\cdot 13 - 5\cdot 5$

Thus, $1 = 13\cdot(2) + 5(-5)$ is a solution.

Thm: $Ax+By=C$ has a solution iff $\gcd(A,B) \mid C$.

[$\Rightarrow$] If $Ax+By=C$ has a solution then

$d \mid A$ and $d \mid B \Rightarrow d \mid C$

Thus, $\gcd(A,B) \mid C$

[$\Leftarrow$] Use the Euclidean Algorithm to solve

$$Ax_1 + By_1 = \gcd(A,B)$$

Write $C = k\gcd(A,B)$ and obtain

$$A(kx_1) + B(ky_1) = C.$$

Ex: Use the Euc. Algo. to solve $107x + 10y = 1$.

$$107 = 10 \cdot 10 + 7$$
$$10 = 1 \cdot 7 + 3$$
$$7 = 2 \cdot 3 + 1$$

Thus,

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= (107 - 10 \cdot 10) - 2(10 - 7) \\ &= (107 - 10 \cdot 10) - 2(10 - [107 - 10 \cdot 10]) \\ &= 3 \cdot 107 - 12 \cdot 10 \end{aligned}$$

Ex: Use the Euc. Algo. to solve $6x + 25y = 7$.

$$25 = 4 \cdot 6 + 1$$
$$6 = 6 \cdot 1 + 0$$

Thus, $\gcd(25, 6) = 1$.

solve $1 = 6x + 25y$

$$1 = 25 - 4 \cdot 6$$

multiply through by 7.

$$7 = 7 \cdot 25 + 6 \cdot (-28)$$

Summary:

- The Euclidean Algorithm (Practice!)
- Solving linear diophantine equations

MAT 2A6 Wk 4b

Ex: Write out the multiplication table mod 4.

·	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

NB: There is no x s.t. $2x \equiv 1 \bmod 4$.

Ex: Write out the mult. table mod 5.

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

NB: There IS x s.t. $2x \equiv 1 \bmod 5$.

Defn: A MULTIPLICATIVE INVERSE of $k \bmod n$ is x such that $kx \equiv 1 \bmod n$.

"What is $\frac{1}{3}$?" $\frac{1}{3}$ is x such that $3x = 1$.

In this sense, $\frac{1}{3} \equiv 2 \bmod 5$ since $2 \cdot 3 \equiv 1 \bmod 5$.

Thm (Inverses are unique)

If $kx \equiv ky \equiv 1 \bmod n$ then $x \equiv y \bmod n$.

Pf: Suppose $kx \equiv 1 \bmod n$ and $ky \equiv 1 \bmod n$.

$ky \equiv 1 \bmod n \Rightarrow xky \equiv x \cdot 1 \bmod n$

\# using $xk \equiv 1 \bmod n$ $\Rightarrow (xk)y \equiv x \bmod n$

$\Rightarrow y \equiv x \bmod n$.

Thm: If $\gcd(a, m) = 1$ then $ax \equiv 1 \bmod m$ has a solution.

Pf: Use the Euclidean algorithm to solve

$$ax + my = 1$$

$$1 \equiv ax + my \equiv ax \bmod m.$$

Thus x is a solution of $ax \equiv 1 \bmod m$.

Ex: Find the inverse of 6 mod 35.

$35 = 5 \cdot 6 + 5$

$6 = 1 \cdot 5 + 1$

Thus, $1 = 6 - 5$

$= 6(35 - 5 \cdot 6)$

$= 6 \cdot 6 - 35$

Thus, $6 \cdot 6 \equiv 1 \bmod 35$

Ex: Find the inverse of 5 mod 14

$14 = 2 \cdot 5 + 4$

$5 = 1 \cdot 4 + 1$

Thus, $1 = 5 - 4$

$= 5 - (14 - 2 \cdot 5)$

$= 3 \cdot 5 - 14$.

Thus $3 \cdot 5 \equiv 1 \bmod 14$

Arithmetic Mod a Prime

Thm (Fermat): If $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$

NB: $p \nmid a \Rightarrow \gcd(a,p) = 1 \Rightarrow aA \equiv 1 \bmod p$

Pf: Consider the set $S = \{1, 2, 3, \cdots, p-1\}$ and the map $x \longmapsto ax \bmod p$ from S to S.

If $ax \equiv ay \bmod p$ then $Aax \equiv Aay \bmod p$
$\Rightarrow x \equiv y \bmod p$.

Since $x, y \leq p-1$ we get $x = y$.

Thus, every element of S gets mapped to a distinct element of S. The map just re-arranges the set S.

Thus,

$$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv (1 \cdot a)(2 \cdot a) \cdots [(p-1) \cdot a]$$
$$\equiv [1 \cdot 2 \cdot 3 \cdots (p-1)] \cdot a^{p-1}$$

cancel $1 \cdot 2 \cdot 3 \cdots (p-1)$ from both sides.

Therefore, $1 \equiv a^{p-1} \bmod p$.

Memorize this proof.

Thm (Wilson) p is prime $\Rightarrow (p-1)! \equiv p-1 \bmod p$.

Pf: If p is prime then $k \leq p-1 \Rightarrow \gcd(k,p)=1$.

Thus, each term in $(p-1)!$ has an inverse.

These cancel in pairs, except $k=1$ and $k=p-1$.

Therefore, $(p-1)! \equiv (p-1) \bmod p$.

E.g: $10! = 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10$

$= (2\cdot 6)\cdot(3\cdot 4)\cdot(5\cdot 9)\cdot(7\cdot 8)\cdot 10$

$\equiv 1\cdot 1\cdot 1\cdot 1\cdot 10 \equiv 11-1 \bmod 11$.

Fact: $(4-1)! \equiv 2 \bmod 4$.

Thm: If $n>4$ is composite then $(n-1)! \equiv 0 \bmod n$.

If $n=pq$ where $p<q$ then $(n-1)! \equiv 1\cdot 2\cdot p\cdots q\cdots(n-1)$
$\equiv 0 \bmod n$

If $n=p^2$ then $1<p<2p\leq n-1$ thus
$(n-1)! = 1\cdot 2\cdot 3\cdots p\cdots(2p)\cdots(n-1)$
$\equiv 0 \bmod n$.

Silly Primality Test: compute $(k-1)! \bmod k$.

If you get 2, then $k=4$. If you get 0, then k is composit
otherwise, k is prime.