

Euclidean Algorithm'

Number Theory in the Elements

1. BookVII-IX (without equations)
va. Euclidean Algorithm
a. Find the GCD of two numbers
b. It shows the GCD of two relatively prime numbers is 1
2. VII.30: prime p, plab implies pla or plb
v 4. VII.31: any composite is divisible by some prime
a. key: well-ordering principle (positive ins)

PROPOSITION IX. 14 If a number be the least that is measured by prime

- 5. numbers, it will not be measured by any other prime number except IX.14: those originally measuring it.
a. Unique Factorization / Fund. Thm. Arithmetic
v. Application: $8^{\wedge} \mathrm{N}$ doesn't end in 0 for any N
i. (if it did, it'd be divisible by 5 , but $8^{\wedge} \mathrm{N}$ is just $2^{\prime}$ 's)
-6. Towards infinitude:
$2,3,5,7,11,13,17,19,23,29,31,37,41,43$,
va. $47,53,59,61,67,71,73,79,83,89,97,101$,
103, 107, 109, 113, 127, 131, 137, 139, 149, 151
i. the first 36,25 of which are less than 100
b. sparsity: between $10,000,001$ and $10,000,100$ there are only 2

3. prime $p, \underbrace{p \mid a b} \Rightarrow$ pla or pl $p$ divides $a b$
means $a b=m p$
prove:
Assume $p l a b$.
If pla wive done.

14,64 - what's the ged

$$
64=14 \cdot 4+8
$$

$$
14=8+1+6
$$

$$
8=6.1+2
$$

$$
6=2.3+0
$$

$$
2=\operatorname{gcd}
$$

108,3
$108=3.36$

$$
\text { BTw: Rel purine } \Rightarrow \exists a, b \in \mathbb{Z}
$$

 sit.

$$
108(a)+5(b)=1
$$

$$
\begin{aligned}
& 108=5 \cdot 21+3 \\
& 5=3.1+2 \\
& 3=2.1+0 \rightarrow \text { Relatively } \\
& 2=111+1
\end{aligned}
$$

If $p$ ta $\Rightarrow \operatorname{gcd}(p, a)=1$ so $p m+a n=1$
( not dinges
Euclid's Lemma: $a b b c_{i}{ }^{\prime} \operatorname{gcd}(a, b)=1$ the $a \mid c$
Bu Euclid's len nat plab ${ }^{\text {q }} \operatorname{gcd}(p, a)=1$ so pleb. (Euclid lemma holds ble:
$\Rightarrow 1=p x+a y$ from
$\Rightarrow b=p b x+a b y$ multiple bs $b$
$\rightarrow$ bu assumption is a milt if $p$

$$
b=p b x+p s y=p(b x+s y)
$$

$b$ is a multiple of $p \quad \therefore \quad p l b$.
Unique Factorization: Any whole number decomposes into a product of primes in exactly ore way

So, if $n \in \mathbb{Z}, \quad n=P_{1} \ldots P_{r} \quad \frac{1}{\xi} \quad P_{i}$ are unique.

Proposition: there are infinite \# of primes.

- This is due to Enctil
- This is perhops surprising.
proof: By contradiction, suppose $\left\{2,3,5,7, \ldots, p_{k}\right\}$ are all the pres. Form $N=2.3,5 \cdot 71 \ldots \cdot P_{k}+1$.
this factors uniquely into a $\underbrace{\text { product of primer, Too. }}$ these are the ores in list

So there is some $P_{i}$ in $m y$ list that divides $N$ $\mathbb{N}=P_{i} \cdot P_{1} \cdot P_{2} \cdot P_{l}$, but $P_{i}$ also divides $2.3 .5 \cdot \ldots \cdot P_{K}$ $\Rightarrow p_{i} \mid N$ and $p_{i} \mid N-1$
$\Rightarrow$ if $p$ divides $a \frac{1}{4} b$ then $p(a-b$
$\Rightarrow p_{i} \mid 1 \times\left(\right.$ all pomes $>1$ 1 $\neq p_{i} \cdot m$ )

Truro kinds of primes, greater then 2.

$$
\begin{array}{rlrl}
p=17=4.4+1 & 13 & =4.3+1 \\
\text { BLUE } & =4.4-3
\end{array}
$$

$4 k+1$

$$
p=31=4 \cdot 7+3
$$

$$
\text { MAGENTA } 4 k+3
$$

$$
\begin{aligned}
11 & =4 \cdot 2+3 \\
& =4(3)-1 \\
19 & =4 \cdot 5-1
\end{aligned}
$$

Ex $\{7,3\} \Longrightarrow 7^{2}=4^{2} 9=4.8+1$


Golden Ratio in Regular Pentagon
The golden ratio, $\phi=\frac{1+\sqrt{5}}{2}$, makes frequent and often unexpected appearance in geometry. Regular pentagon -
the pentagram - is one of the places where the golden ratio appears in abundance.


To mention a few (some of which have been proved elsewhere, others are straightforward):

$$
\frac{D E}{E X}=\frac{E X}{X Y}=\frac{U V}{X Y}=\frac{E Y}{E X}=\frac{B E}{A E}=\phi
$$

$\cos \left(\frac{2 \pi}{5}\right)=1.618 \ldots$ golden ratio


$$
\begin{aligned}
5 \alpha & =360 \\
\alpha=\frac{2 \pi}{S} & =72^{\circ}
\end{aligned}
$$

