CS250: Discrete Math for Computer Science

L17: Euclid's Algorithm

Factoring integers is computationally difficult

To factor a thousand-bit integer, a,

we would try all divisors up to $\sqrt{a}$

but that would be about 2^{500} possible divisors!

This is **exponential time** with the size of the input, so it is **not feasible**.

Next, we will see how over 2300 years ago, Euclid gave a **very efficient algorithm** to compute $\gcd(a, b)$, without factoring.

This was in Euclid's Geometry text. He was thinking about line segments and wanted to be able to compute the length d of the longest line segment that evenly divided two given line segments, a and b.

Euclid's algorithm

To compute: $\gcd(12, 18) = \gcd(18, 12)$,

Divide the bigger number, **b**, by the smaller, **s**, computing the remainder, **r**

$$\begin{aligned} \mathbf{18} &= 1 \cdot \mathbf{12} + \mathbf{6} \\ \mathbf{12} &= 2 \cdot \mathbf{6} + 0 \end{aligned}$$

Answer: $\gcd(18, 12) = \mathbf{6}$

Euclid's algorithm

Compute: $\gcd(123, 42)$

$$\begin{aligned} 123 &= 2 \cdot 42 + 39 \\ 42 &= 1 \cdot 39 + 3 \\ 39 &= 13 \cdot 3 + 0 \end{aligned}$$

Answer: $\gcd(123, 42) = 3$

Compute: $\gcd(13, 8)$

$$\begin{aligned} 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Answer: $\gcd(13, 8) = 1$

Euclid's Algorithm: Why It Works

Algorithm **gcd**(b, s)
Input: integers $b > s \geq 0$

1. **while** $(s \neq 0) : \{\ b := s; \quad s := (b \,\%\, s)\ \}$
2. **return**(b) # $\gcd(b, 0) = b$

Euclid's Algorithm: Why It Works

Algorithm **gcd**(b, s)
Input: integers $b > s \geq 0$

1. **while** $(s \neq 0) : \{\ b := s; \quad s := (b \,\%\, s)\ \}$
2. **return**(b) # $\gcd(b, 0) = b$

Lemma [Euclid, 300 B.C.]

If $b > s > 0$ **Then** $\gcd(b, s) = \gcd(s, (b \,\%\, s))$

Euclid's Algorithm: Why It Works

Algorithm **gcd**(b, s)
Input: integers $b > s \geq 0$

1. **while** $(s \neq 0) : \{\ b := s; \quad s := (b \,\%\, s)\ \}$
2. **return**(b) # $\gcd(b, 0) = b$

Lemma [Euclid, 300 B.C.]

If $b > s > 0$ **Then** $\gcd(b, s) = \gcd(s, (b \,\%\, s))$

Proof: Let $r = b \,\%\, s$ $b = q \cdot s + r$

Euclid's Algorithm: Why It Works

Algorithm **gcd**(b, s)
Input: integers $b > s \geq 0$

1. **while** $(s \neq 0) : \{\ b := s; \quad s := (b \,\%\, s)\ \}$
2. **return**(b) # $\gcd(b, 0) = b$

Lemma [Euclid, 300 B.C.]
If $b > s > 0$ **Then** $\gcd(b, s) = \gcd(s, (b \,\%\, s))$

Proof: Let $r = b \,\%\, s$ $b = q \cdot s + r$

$\forall d\ (d|b \wedge d|s \quad \leftrightarrow \quad d|s \wedge d|r)$

Euclid's Algorithm: Why It Works

Algorithm **gcd**(b, s)
Input: integers $b > s \geq 0$

1. **while** $(s \neq 0) : \{\ b := s; \quad s := (b \,\%\, s)\ \}$
2. **return**(b) # $\gcd(b, 0) = b$

Lemma [Euclid, 300 B.C.]
If $b > s > 0$ **Then** $\gcd(b, s) = \gcd(s, (b \,\%\, s))$

Proof: Let $r = b \,\%\, s$ $b = q \cdot s + r$

$\forall d\ (d|b \wedge d|s \quad \leftrightarrow \quad d|s \wedge d|r)$

Thus, $\gcd(b, s) \ = \ \gcd(s, r) \ = \ \gcd(b', s')$.

Euclid's Algorithm: Why It Works

Algorithm **gcd**(b, s)
Input: integers $b > s \geq 0$

1. **while** $(s \neq 0)$: { $b := s$; $s := (b \,\%\, s)$ }
2. **return**(b) # $\gcd(b, 0) = b$

Lemma [Euclid, 300 B.C.]
If $b > s > 0$ **Then** $\gcd(b, s) = \gcd(s, (b \,\%\, s))$

Proof: Let $r = b \,\%\, s$ $b = q \cdot s + r$

$\forall d \; (d|b \wedge d|s \quad \leftrightarrow \quad d|s \wedge d|r)$

Thus, $\gcd(b, s) \; = \; \gcd(s, r) \; = \; \gcd(b', s')$.

Note: $\text{length}(b') + \text{length}(s') \; < \; \text{length}(b) + \text{length}(s)$

Euclid's Algorithm: Why It Works

Algorithm **gcd**(b, s)
Input: integers $b > s \geq 0$

1. **while** $(s \neq 0)$: { $b := s$; $s := (b \,\%\, s)$ }
2. **return**(b) # $\gcd(b, 0) = b$

Lemma [Euclid, 300 B.C.]
If $b > s > 0$ **Then** $\gcd(b, s) = \gcd(s, (b \,\%\, s))$

Proof: Let $r = b \,\%\, s$ $b = q \cdot s + r$

$\forall d \; (d|b \wedge d|s \quad \leftrightarrow \quad d|s \wedge d|r)$

Thus, $\gcd(b, s) \; = \; \gcd(s, r) \; = \; \gcd(b', s')$.

Note: $\text{length}(b') + \text{length}(s') \; < \; \text{length}(b) + \text{length}(s)$

Euclid's Algorithm correctly computes the **gcd** of its inputs in at most $\text{length}(b) + \text{length}(s)$ rounds. □

Euclid's Algorithm: Why It Works

Algorithm $\gcd(b, s)$
Input: integers $b > s \geq 0$

1. **while** $(s \neq 0)$: { $b := s$; $s := (b \,\%\, s)$ }
2. **return**(b) # $\gcd(b, 0) = b$

Lemma [Euclid, 300 B.C.]
If $b > s > 0$ **Then** $\gcd(b, s) = \gcd(s, (b \,\%\, s))$

Proof: Let $r = b \,\%\, s$ $b = q \cdot s + r$

$\forall d \; (d|b \wedge d|s \quad \leftrightarrow \quad d|s \wedge d|r)$

Thus, $\gcd(b, s) \;=\; \gcd(s, r) \;=\; \gcd(b', s')$.

Note: $\text{length}(b') + \text{length}(s') \;<\; \text{length}(b) + \text{length}(s)$

Euclid's Algorithm correctly computes the **gcd** of its inputs in at most $\text{length}(b) + \text{length}(s)$ rounds. □

$$\text{length}(n) \;=\; \text{length of } n \text{ in binary} \;=\; \lceil 1 + \log n \rceil$$

Write gcd(a, b) as a linear combination of a and b

Thm. $\forall a\, b\, \exists x\, y \quad a \cdot x + b \cdot y \;=\; \gcd(a, b)$

Write gcd(a, b) as a linear combination of a and b

Thm. $\forall a\, b\, \exists x\, y \quad a \cdot x + b \cdot y \;=\; \gcd(a, b)$

Proof: We can compute x and y from a and b by running **Euclid's Algorithm Backwards**. □

Write gcd(a, b) as a linear combination of a and b

Thm. $\forall a\, b\, \exists x\, y \quad a \cdot x + b \cdot y = \gcd(a, b)$

Proof: We can compute x and y from a and b by running **Euclid's Algorithm Backwards**. □

$$\mathbf{18} = 1 \cdot \mathbf{12} + \mathbf{6} = \gcd(18, 12)$$

Write gcd(a, b) as a linear combination of a and b

Thm. $\forall a\, b\, \exists x\, y \quad a \cdot x + b \cdot y = \gcd(a, b)$

Proof: We can compute x and y from a and b by running **Euclid's Algorithm Backwards**. □

$$\mathbf{18} = 1 \cdot \mathbf{12} + \mathbf{6} = \gcd(18, 12)$$

$$\mathbf{6} = \mathbf{18} \cdot 1 + \mathbf{12} \cdot (-1)$$

Write gcd(a, b) as a linear combination of a and b

$$\begin{aligned} \mathbf{123} &= 2 \cdot \mathbf{42} + \mathbf{39} \\ \mathbf{42} &= 1 \cdot \mathbf{39} + \mathbf{3} \qquad = \gcd(\mathbf{123}, \mathbf{42}) \end{aligned}$$

Write gcd(a, b) as a linear combination of a and b

$$\begin{aligned} \mathbf{123} &= 2 \cdot \mathbf{42} + \mathbf{39} \\ \mathbf{42} &= 1 \cdot \mathbf{39} + \mathbf{3} \qquad = \gcd(\mathbf{123}, \mathbf{42}) \end{aligned}$$

express gcd(a, b); **regroup**; **repeat**.

Write gcd(a, b) as a linear combination of a and b

$$\begin{aligned} \mathbf{123} &= 2 \cdot \mathbf{42} + \mathbf{39} \\ \mathbf{42} &= 1 \cdot \mathbf{39} + \mathbf{3} \qquad = \gcd(\mathbf{123}, \mathbf{42}) \end{aligned}$$

express gcd(a, b); **regroup**; **repeat**.

$$\mathbf{3} = \mathbf{42} \cdot 1 + \mathbf{39} \cdot (-1)$$

Write gcd(a, b) as a linear combination of a and b

$$\begin{aligned} \mathbf{123} &= 2\cdot \mathbf{42} + \mathbf{39} \\ \mathbf{42} &= 1\cdot \mathbf{39} + \mathbf{3} \qquad = \gcd(\mathbf{123}, \mathbf{42}) \end{aligned}$$

express gcd(a, b); **regroup**; **repeat**.

$$\begin{aligned} \mathbf{3} &= \mathbf{42}\cdot 1 + \mathbf{39}\cdot(-1) \\ \mathbf{3} &= \mathbf{42}\cdot 1 + (\mathbf{123} + \mathbf{42}\cdot(-2))\cdot(-1) \end{aligned}$$

Write gcd(a, b) as a linear combination of a and b

$$\begin{aligned} \mathbf{123} &= 2\cdot\mathbf{42} + \mathbf{39} \\ \mathbf{42} &= 1\cdot\mathbf{39} + \mathbf{3} = \gcd(\mathbf{123},\mathbf{42}) \end{aligned}$$

express gcd(a, b); **regroup**; **repeat**.

$$\begin{aligned} \mathbf{3} &= \mathbf{42}\cdot 1 + \mathbf{39}\cdot(-1) \\ \mathbf{3} &= \mathbf{42}\cdot 1 + (\mathbf{123}+\mathbf{42}\cdot(-2))\cdot(-1) \\ \mathbf{3} &= \mathbf{123}\cdot(-1) + \mathbf{42}\cdot 3 \end{aligned}$$

Write gcd(a, b) as a linear combination of a and b

$$\begin{aligned} \mathbf{123} &= 2 \cdot \mathbf{42} + \mathbf{39} \\ \mathbf{42} &= 1 \cdot \mathbf{39} + \mathbf{3} \qquad = \gcd(\mathbf{123}, \mathbf{42}) \end{aligned}$$

express gcd(a, b); **regroup**; **repeat**.

$$\begin{aligned} \mathbf{3} &= \mathbf{42} \cdot 1 + \mathbf{39} \cdot (-1) \\ \mathbf{3} &= \mathbf{42} \cdot 1 + (\mathbf{123} + \mathbf{42} \cdot (-2)) \cdot (-1) \\ \mathbf{3} &= \mathbf{123} \cdot (-1) + \mathbf{42} \cdot 3 \end{aligned}$$

Check: $-123 + 126 = 3$

Write gcd(a, b) as a linear combination of a and b

$$\begin{aligned}
\mathbf{13} &= 1 \cdot 8 + \mathbf{5} \\
\mathbf{8} &= 1 \cdot 5 + \mathbf{3} \\
\mathbf{5} &= 1 \cdot 3 + \mathbf{2} \\
\mathbf{3} &= 1 \cdot 2 + \mathbf{1} \qquad = \quad \gcd(13, 8)
\end{aligned}$$

express gcd(a, b); **regroup**; **repeat**.

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

$$\begin{aligned}
\mathbf{1} &= 5 \cdot (-1) + 3 \cdot 2 \\
\mathbf{1} &= 5 \cdot (-1) + (8 + 5 \cdot (-1)) \cdot 2
\end{aligned}$$

$$\begin{aligned}
\mathbf{1} &= 8 \cdot (2) + 5 \cdot -3 \\
\mathbf{1} &= 8 \cdot (2) + (13 + 8 \cdot (-1)) \cdot -3
\end{aligned}$$

$$\mathbf{1} = 13 \cdot (-3) + 8 \cdot 5$$

Don't forget to check: $1 = -39 + 40$

Multipicative Inverses mod m

Cor. If $\gcd(a, m) = 1$, we can **efficiently** compute $a^{-1} \bmod m$.

Multipicative Inverses mod m

Cor. If $\gcd(a, m) = 1$, we can **efficiently** compute $a^{-1} \bmod m$.

Proof: Compute x, y, s.t. $a \cdot x + m \cdot y = \gcd(a, m) = 1$.

Multipicative Inverses mod m

Cor. If $\gcd(a, m) = 1$, we can **efficiently** compute $a^{-1} \bmod m$.

Proof: Compute x, y, s.t. $a \cdot x + m \cdot y = \gcd(a, m) = 1$.

$$a \cdot x = 1 - m \cdot y \equiv 1 \pmod{m}$$

Multipicative Inverses mod m

Cor. If $\gcd(a, m) = 1$, we can **efficiently** compute $a^{-1} \bmod m$.

Proof: Compute x, y, s.t. $a \cdot x + m \cdot y = \gcd(a, m) = 1$.

$a \cdot x = 1 - m \cdot y \equiv 1 \pmod{m}$

$x = a^{-1} \bmod m$ □

Multipicative Inverses mod m

Cor. If $\gcd(a, m) = 1$, we can **efficiently** compute $a^{-1} \bmod m$.

Proof: Compute x, y, s.t. $a \cdot x + m \cdot y = \gcd(a, m) = 1$.

$a \cdot x = 1 - m \cdot y \equiv 1 \pmod{m}$

$x = a^{-1} \bmod m$ □

Cor. $a^{-1} \bmod m$ exists iff $\gcd(a, m) = 1$.

Multipicative Inverses mod m

Cor. If $\gcd(a, m) = 1$, we can **efficiently** compute $a^{-1} \bmod m$.

Proof: Compute x, y, s.t. $a \cdot x + m \cdot y = \gcd(a, m) = 1$.

$a \cdot x = 1 - m \cdot y \equiv 1 \pmod{m}$

$x = a^{-1} \bmod m$ □

Cor. $a^{-1} \bmod m$ exists iff $\gcd(a, m) = 1$.

Cor. [Jordan-Rachit Thm] $\mathbf{Z}/m\mathbf{Z}$ is a field iff m is prime.

Multipicative Inverses mod m

Cor. If $\gcd(a, m) = 1$, we can **efficiently** compute $a^{-1} \bmod m$.

Proof: Compute x, y, s.t. $a \cdot x + m \cdot y = \gcd(a, m) = 1$.

$$a \cdot x = 1 - m \cdot y \equiv 1 \pmod{m}$$

$$x = a^{-1} \bmod m$$

□

Cor. $a^{-1} \bmod m$ exists iff $\gcd(a, m) = 1$.

Cor. [Jordan-Rachit Thm] $\mathbf{Z}/m\mathbf{Z}$ is a field iff m is prime.

Details in hw3

$a^{-1} \bmod m$ exists iff $\gcd(a, m) = 1$

$\cdot_{\mathbb{Z}/6\mathbb{Z}}$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$a^{-1} \bmod m$ exists iff $\gcd(a, m) = 1$

$\cdot Z/6Z$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Def. $\mathbf{Z}_m^*$ is the **multiplicative group mod m**.

$a^{-1} \bmod m$ exists iff $\gcd(a, m) = 1$

$\cdot^{Z/6Z}$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Def. $\mathbf{Z}_m^*$ is the **multiplicative group mod m**.

$$|\mathbf{Z}_m^*| \;=\; \{a \in \mathbf{Z}/m\mathbf{Z} \;\mid\; \gcd(a, m) = 1\} \qquad x \cdot^{Z_m^*} y \;=\; (x \cdot y) \,\%\, m$$

$a^{-1} \bmod m$ exists iff $\gcd(a, m) = 1$

$\cdot^{Z/6Z}$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Def. $\mathbf{Z}_m^*$ is the **multiplicative group mod m**.

$$|\mathbf{Z}_m^*| = \{a \in \mathbf{Z}/m\mathbf{Z} \mid \gcd(a, m) = 1\} \qquad x \cdot^{Z_m^*} y = (x \cdot y) \,\%\, m$$

$$|\mathbf{Z}_6^*| = \{1, 5\}$$

$\cdot^{Z_6^*}$	1	5
1	1	5
5	5	1

$\mathbf{Z}_m^*$ is the multiplicative group mod m

$$|\mathbf{Z}_5^\star| = \{1, 2, 3, 4\}$$

$.Z_5^\star$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Groups

$$\Sigma_{\text{group}} \stackrel{\text{def}}{=} (;1,\cdot[\text{infix}]^{2},^{-1}[\text{postfix}]^{1})$$

Groups

$$\Sigma_{\text{group}} \stackrel{\text{def}}{=} (;1,\cdot[\text{infix}]^{2},^{-1}[\text{postfix}]^{1})$$

$$G_1 \quad = \quad \forall x\, y\, z \quad x \cdot (y \cdot z) \;=\; (x \cdot y) \cdot z \qquad \textit{associative}$$

Groups

$$\Sigma_{\text{group}} \stackrel{\text{def}}{=} (;1,\cdot\,[\text{infix}]^2,^{-1}\,[\text{postfix}]^1)$$

$$G_1 \quad = \quad \forall x\, y\, z \quad x \cdot (y \cdot z) \;=\; (x \cdot y) \cdot z \qquad \textit{associative}$$

$$G_2 \quad = \quad \forall x \quad x \cdot 1 = x \qquad \textit{identity}$$

Groups

$$\Sigma_{\text{group}} \stackrel{\text{def}}{=} (;1, \cdot[\text{infix}]^{2}, ^{-1}[\text{postfix}]^{1})$$

G_1	$=$	$\forall x\, y\, z \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$	*associative*
G_2	$=$	$\forall x \quad x \cdot 1 = x$	*identity*
G_3	$=$	$\forall x \quad x \cdot x^{-1} = 1$	*inverses*

Groups

$$\Sigma_{\text{group}} \stackrel{\text{def}}{=} (;1, \cdot[\text{infix}]^2, ^{-1}[\text{postfix}]^1)$$

$$\begin{array}{lcll} G_1 & = & \forall x\, y\, z \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z & \textit{associative} \\ G_2 & = & \forall x \quad x \cdot 1 = x & \textit{identity} \\ G_3 & = & \forall x \quad x \cdot x^{-1} = 1 & \textit{inverses} \end{array}$$

Def. A **group** is a $G \in \text{World}[\Sigma_{\text{group}}]$ s.t. $G \models G_1 \wedge G_2 \wedge G_3$.

Groups

$$\Sigma_{\text{group}} \stackrel{\text{def}}{=} (;1, \cdot[\text{infix}]^{2}, ^{-1}[\text{postfix}]^{1})$$

G_1	$=$	$\forall x\, y\, z \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$	*associative*
G_2	$=$	$\forall x \quad x \cdot 1 = x$	*identity*
G_3	$=$	$\forall x \quad x \cdot x^{-1} = 1$	*inverses*

Def. A **group** is a $G \in \text{World}[\Sigma_{\text{group}}]$ s.t. $G \models G_1 \wedge G_2 \wedge G_3$.

Prop. For all $m > 1$, $\quad Z_m^*$ is a group.

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m		

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2		

iClicker 17.1
What is $\varphi(2)$?

A: 1 **B: 2**

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3		

iClicker 17.2

What is $\varphi(3)$?

A: 1 **B: 2**

C: 3

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4		

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5		

iClicker 17.3
What is $\varphi(5)$?

A: 1 B: 2
C: 3 D: 4

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6		

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7		

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8		

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	$\{1, 3, 5, 7\}$

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	$\{1, 3, 5, 7\}$
9		

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	$\{1, 3, 5, 7\}$
9	6	

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	$\{1, 3, 5, 7\}$
9	6	$\{1, 2, 4, 5, 7, 8\}$

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	$\{1, 3, 5, 7\}$
9	6	$\{1, 2, 4, 5, 7, 8\}$
10		

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	$\{1, 3, 5, 7\}$
9	6	$\{1, 2, 4, 5, 7, 8\}$
10	4	

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	$\{1, 3, 5, 7\}$
9	6	$\{1, 2, 4, 5, 7, 8\}$
10	4	$\{1, 3, 7, 9\}$

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	$\{1, 3, 5, 7\}$
9	6	$\{1, 2, 4, 5, 7, 8\}$
10	4	$\{1, 3, 7, 9\}$
11		

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	$\{1, 3, 5, 7\}$
9	6	$\{1, 2, 4, 5, 7, 8\}$
10	4	$\{1, 3, 7, 9\}$
11	10	

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	$\{1, 3, 5, 7\}$
9	6	$\{1, 2, 4, 5, 7, 8\}$
10	4	$\{1, 3, 7, 9\}$
11	10	$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	$\{1, 3, 5, 7\}$
9	6	$\{1, 2, 4, 5, 7, 8\}$
10	4	$\{1, 3, 7, 9\}$
11	10	$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
12		

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	$\{1, 3, 5, 7\}$
9	6	$\{1, 2, 4, 5, 7, 8\}$
10	4	$\{1, 3, 7, 9\}$
11	10	$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
12	4	

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\left\{a \in \mathbf{Z}/m\mathbf{Z} \;\middle|\; \gcd(a, m) = 1\right\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	$\{1, 3, 5, 7\}$
9	6	$\{1, 2, 4, 5, 7, 8\}$
10	4	$\{1, 3, 7, 9\}$
11	10	$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
12	4	$\{1, 5, 7, 11\}$