Some Solutions to HW02 Problems

BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

HW02, Problem 2

We used a generalization of this problem in RSA.

HW02, Problem 2

We used a generalization of this problem in RSA.

So we are going over it.

HW02, Problem 2a, 2b

2a) How many numbers in $\{1, \ldots, 143\}$ have 11 as a factor?

HW02, Problem 2a, 2b

2a) How many numbers in $\{1, \ldots, 143\}$ have 11 as a factor?

Note that $\frac{143}{11} = 13$.

HW02, Problem 2a, 2b

2a) How many numbers in $\{1, \ldots, 143\}$ have 11 as a factor?

Note that $\frac{143}{11} = 13$. 1×11, ..., 13×11 have 11 as factor.

HW02, Problem 2a, 2b

2a) How many numbers in $\{1, \ldots, 143\}$ have 11 as a factor?

Note that $\frac{143}{11} = 13$. 1×11, ..., 13×11 have 11 as factor.
So the answer is 13.

HW02, Problem 2a, 2b

2a) How many numbers in $\{1, \ldots, 143\}$ have 11 as a factor?

Note that $\frac{143}{11} = 13$. 1×11, ..., 13×11 have 11 as factor. So the answer is 13.

2b) How many numbers in $\{1, \ldots, 143\}$ have 13 as a factor?

HW02, Problem 2a, 2b

2a) How many numbers in $\{1, \ldots, 143\}$ have 11 as a factor?

Note that $\frac{143}{11} = 13$. 1×11, ..., 13×11 have 11 as factor.
So the answer is 13.

2b) How many numbers in $\{1, \ldots, 143\}$ have 13 as a factor? 11.

HW02, Problem 2a, 2b

2a) How many numbers in $\{1, \ldots, 143\}$ have 11 as a factor?

Note that $\frac{143}{11} = 13$. 1×11, …, 13×11 have 11 as factor.
So the answer is 13.

2b) How many numbers in $\{1, \ldots, 143\}$ have 13 as a factor? 11.

Generalize How many in $\{1, \ldots, ab\}$ have a as a factor?

HW02, Problem 2a, 2b

2a) How many numbers in $\{1, \ldots, 143\}$ have 11 as a factor?

Note that $\frac{143}{11} = 13$. 1×11, ..., 13×11 have 11 as factor.
So the answer is 13.

2b) How many numbers in $\{1, \ldots, 143\}$ have 13 as a factor? 11.

Generalize How many in $\{1, \ldots, ab\}$ have a as a factor? b.

HW02, Problem 2c, 2d

2c) How many in $\{1, \ldots, 143\}$ have 11 & 13 as a factor?

HW02, Problem 2c, 2d

2c) How many in $\{1, \ldots, 143\}$ have 11 & 13 as a factor?

11,13 are rel prime, so any such num is mult of $11 = 143$. Only 1.

HW02, Problem 2c, 2d

2c) How many in $\{1, \ldots, 143\}$ have 11 & 13 as a factor?

11,13 are rel prime, so any such num is mult of $11 = 143$. Only 1.

2d) Using 2a,2b,2c, and law of inc-excl, to find $\phi(143)$.

HW02, Problem 2c, 2d

2c) How many in $\{1, \ldots, 143\}$ have 11 & 13 as a factor?

11,13 are rel prime, so any such num is mult of $11 = 143$. Only 1.

2d) Using 2a,2b,2c, and law of inc-excl, to find $\phi(143)$.
$A = \{x \in \{1, \ldots, 143\} : x \equiv 0 \pmod{11}\}$. By 2a, $|A| = 13$.

HW02, Problem 2c, 2d

2c) How many in $\{1, \ldots, 143\}$ have 11 & 13 as a factor?

11,13 are rel prime, so any such num is mult of $11 = 143$. Only 1.

2d) Using 2a,2b,2c, and law of inc-excl, to find $\phi(143)$.
$A = \{x \in \{1, \ldots, 143\} \colon x \equiv 0 \pmod{11}\}$. By 2a, $|A| = 13$.
$B = \{x \in \{1, \ldots, 143\} \colon x \equiv 0 \pmod{13}\}$. By 2b, $|B| = 11$.

HW02, Problem 2c, 2d

2c) How many in $\{1, \ldots, 143\}$ have 11 & 13 as a factor?

11,13 are rel prime, so any such num is mult of $11 = 143$. Only 1.

2d) Using 2a,2b,2c, and law of inc-excl, to find $\phi(143)$.
$A = \{x \in \{1, \ldots, 143\} \colon x \equiv 0 \pmod{11}\}$. By 2a, $|A| = 13$.
$B = \{x \in \{1, \ldots, 143\} \colon x \equiv 0 \pmod{13}\}$. By 2b, $|B| = 11$.
By 2c, $|A \cap B| = 1$.

HW02, Problem 2c, 2d

2c) How many in $\{1, \ldots, 143\}$ have 11 & 13 as a factor?

11,13 are rel prime, so any such num is mult of $11 = 143$. Only 1.

2d) Using 2a,2b,2c, and law of inc-excl, to find $\phi(143)$.
$A = \{x \in \{1, \ldots, 143\} : x \equiv 0 \pmod{11}\}$. By 2a, $|A| = 13$.
$B = \{x \in \{1, \ldots, 143\} : x \equiv 0 \pmod{13}\}$. By 2b, $|B| = 11$.
By 2c, $|A \cap B| = 1$.
Numbers NOT rel prime to 143 have 11 or 13 as a factor. By law of inc-exc there are

$$|A| + |B| - |A \cup B| = 13 + 11 - 1 = 23 \text{ such numbers}$$

HW02, Problem 2c, 2d

2c) How many in $\{1, \ldots, 143\}$ have 11 & 13 as a factor?

11,13 are rel prime, so any such num is mult of $11 = 143$. Only 1.

2d) Using 2a,2b,2c, and law of inc-excl, to find $\phi(143)$.
$A = \{x \in \{1, \ldots, 143\} : x \equiv 0 \pmod{11}\}$. By 2a, $|A| = 13$.
$B = \{x \in \{1, \ldots, 143\} : x \equiv 0 \pmod{13}\}$. By 2b, $|B| = 11$.
By 2c, $|A \cap B| = 1$.
Numbers NOT rel prime to 143 have 11 or 13 as a factor. By law of inc-exc there are

$$|A| + |B| - |A \cup B| = 13 + 11 - 1 = 23 \text{ such numbers}$$

Hence there are $143 - 23 = 120$ that are NOT rel prime to 143.

HW02, Problem 2c, 2d

2c) How many in $\{1, \ldots, 143\}$ have 11 & 13 as a factor?

11,13 are rel prime, so any such num is mult of $11 = 143$. Only 1.

2d) Using 2a,2b,2c, and law of inc-excl, to find $\phi(143)$.
$A = \{x \in \{1, \ldots, 143\} : x \equiv 0 \pmod{11}\}$. By 2a, $|A| = 13$.
$B = \{x \in \{1, \ldots, 143\} : x \equiv 0 \pmod{13}\}$. By 2b, $|B| = 11$.
By 2c, $|A \cap B| = 1$.
Numbers NOT rel prime to 143 have 11 or 13 as a factor. By law of inc-exc there are

$$|A| + |B| - |A \cup B| = 13 + 11 - 1 = 23 \text{ such numbers}$$

Hence there are $143 - 23 = 120$ that are NOT rel prime to 143.
So $\phi(143) = 120$.

HW02, Problem 2e

2e) Give a formula for $\phi(pq)$ where p, q are primes.

HW02, Problem 2e

2e) Give a formula for $\phi(pq)$ where p, q are primes.

How many numbers in $\{1, \ldots, pq\}$ have p as a factor?

HW02, Problem 2e

2e) Give a formula for $\phi(pq)$ where p, q are primes.

How many numbers in $\{1, \ldots, pq\}$ have p as a factor? q.

HW02, Problem 2e

2e) Give a formula for $\phi(pq)$ where p, q are primes.

How many numbers in $\{1, \ldots, pq\}$ have p as a factor? q.

How many numbers in $\{1, \ldots, pq\}$ have q as a factor?

HW02, Problem 2e

2e) Give a formula for $\phi(pq)$ where p, q are primes.

How many numbers in $\{1, \ldots, pq\}$ have p as a factor? q.

How many numbers in $\{1, \ldots, pq\}$ have q as a factor? p.

HW02, Problem 2e

2e) Give a formula for $\phi(pq)$ where p, q are primes.

How many numbers in $\{1, \ldots, pq\}$ have p as a factor? q.

How many numbers in $\{1, \ldots, pq\}$ have q as a factor? p.

How many in $\{1, \ldots, pq\}$ have p & q as factors

HW02, Problem 2e

2e) Give a formula for $\phi(pq)$ where p, q are primes.

How many numbers in $\{1, \ldots, pq\}$ have p as a factor? q.

How many numbers in $\{1, \ldots, pq\}$ have q as a factor? p.

How many in $\{1, \ldots, pq\}$ have p & q as factors 1.

HW02, Problem 2e

2e) Give a formula for $\phi(pq)$ where p, q are primes.

How many numbers in $\{1, \ldots, pq\}$ have p as a factor? q.

How many numbers in $\{1, \ldots, pq\}$ have q as a factor? p.

How many in $\{1, \ldots, pq\}$ have p & q as factors 1.
$A = \{x \in \{1, \ldots, pq\} \colon x \equiv 0 \pmod{p}\}$. $|A| = q$.

HW02, Problem 2e

2e) Give a formula for $\phi(pq)$ where p, q are primes.

How many numbers in $\{1, \ldots, pq\}$ have p as a factor? q.

How many numbers in $\{1, \ldots, pq\}$ have q as a factor? p.

How many in $\{1, \ldots, pq\}$ have p & q as factors 1.
$A = \{x \in \{1, \ldots, pq\} \colon x \equiv 0 \pmod{p}\}$. $|A| = q$.
$B = \{x \in \{1, \ldots, pq\} \colon x \equiv 0 \pmod{q}\}$. $|B| = p$.

HW02, Problem 2e

2e) Give a formula for $\phi(pq)$ where p, q are primes.

How many numbers in $\{1, \ldots, pq\}$ have p as a factor? q.

How many numbers in $\{1, \ldots, pq\}$ have q as a factor? p.

How many in $\{1, \ldots, pq\}$ have p & q as factors 1.
$A = \{x \in \{1, \ldots, pq\} \colon x \equiv 0 \pmod{p}\}$. $|A| = q$.
$B = \{x \in \{1, \ldots, pq\} \colon x \equiv 0 \pmod{q}\}$. $|B| = p$.
$|A \cap B| = 1$.

HW02, Problem 2e

2e) Give a formula for $\phi(pq)$ where p, q are primes.

How many numbers in $\{1, \ldots, pq\}$ have p as a factor? q.

How many numbers in $\{1, \ldots, pq\}$ have q as a factor? p.

How many in $\{1, \ldots, pq\}$ have p & q as factors 1.
$A = \{x \in \{1, \ldots, pq\} \colon x \equiv 0 \pmod{p}\}$. $|A| = q$.
$B = \{x \in \{1, \ldots, pq\} \colon x \equiv 0 \pmod{q}\}$. $|B| = p$.
$|A \cap B| = 1$.
Nums NOT rel prime to pq have p or q as factor. By inc-exc there are

$$|A| + |B| - |A \cap B| = p + q - 1 \text{ such numbers}$$

HW02, Problem 2e

2e) Give a formula for $\phi(pq)$ where p, q are primes.

How many numbers in $\{1, \ldots, pq\}$ have p as a factor? q.

How many numbers in $\{1, \ldots, pq\}$ have q as a factor? p.

How many in $\{1, \ldots, pq\}$ have p & q as factors 1.
$A = \{x \in \{1, \ldots, pq\} : x \equiv 0 \pmod{p}\}$. $|A| = q$.
$B = \{x \in \{1, \ldots, pq\} : x \equiv 0 \pmod{q}\}$. $|B| = p$.
$|A \cap B| = 1$.
Nums NOT rel prime to pq have p or q as factor. By inc-exc there are

$$|A| + |B| - |A \cap B| = p + q - 1 \text{ such numbers}$$

There are $p + q - 1$ that are NOT rel prime to 143.

HW02, Problem 2e

2e) Give a formula for $\phi(pq)$ where p, q are primes.

How many numbers in $\{1, \ldots, pq\}$ have p as a factor? q.

How many numbers in $\{1, \ldots, pq\}$ have q as a factor? p.

How many in $\{1, \ldots, pq\}$ have p & q as factors 1.
$A = \{x \in \{1, \ldots, pq\} : x \equiv 0 \pmod{p}\}$. $|A| = q$.
$B = \{x \in \{1, \ldots, pq\} : x \equiv 0 \pmod{q}\}$. $|B| = p$.
$|A \cap B| = 1$.
Nums NOT rel prime to pq have p or q as factor. By inc-exc there are

$$|A| + |B| - |A \cap B| = p + q - 1 \text{ such numbers}$$

There are $p + q - 1$ that are NOT rel prime to 143. So there are

HW02, Problem 2e

2e) Give a formula for $\phi(pq)$ where p, q are primes.

How many numbers in $\{1, \ldots, pq\}$ have p as a factor? q.

How many numbers in $\{1, \ldots, pq\}$ have q as a factor? p.

How many in $\{1, \ldots, pq\}$ have p & q as factors 1.
$A = \{x \in \{1, \ldots, pq\} : x \equiv 0 \pmod{p}\}$. $|A| = q$.
$B = \{x \in \{1, \ldots, pq\} : x \equiv 0 \pmod{q}\}$. $|B| = p$.
$|A \cap B| = 1$.
Nums NOT rel prime to pq have p or q as factor. By inc-exc there are

$$|A| + |B| - |A \cap B| = p + q - 1 \text{ such numbers}$$

There are $p + q - 1$ that are NOT rel prime to 143. So there are

$$\phi(pq) = pq - (p + q - 1) = pq - p - q + 1 = (p - 1)(q - 1) = \phi(p)\phi(q)$$