Number Theory

ITT9131 Konkreete Matemaatika

Contents

Next section

Congruences

Definition

Integer a is congruent to integer b modulo $m > 0$, if a and b give the same remainder when divided by m. Notation $a \equiv b \pmod{m}$.

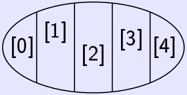
Alternative definition: $a \equiv b \pmod{m}$ iff $m|(b-a)$. Congruence is

a *equivalence relation:*

Reflectivity: $a \equiv a \pmod{m}$

Symmetry: $a \equiv b \pmod{m} \quad \Rightarrow \quad b \equiv a \pmod{m}$

Transitivity: $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m} \quad \Rightarrow \quad a \equiv c \pmod{m}$



Properties of the congruence relation

- If $a \equiv b \pmod{m}$ and $d|m$, then $a \equiv b \pmod{d}$
- If $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, then $a \equiv b \pmod{lcm(m_1, m_2, \ldots, m_k)}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
- If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{m}$ for any integer k
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$
- If $a \equiv b \pmod{m}$, then $a + um \equiv b + vm \pmod{m}$ for every integers u and v
- If $ka \equiv kb \pmod{m}$ and $gcd(k, m) = 1$, then $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$ iff $ak \equiv bk \pmod{mk}$ for any natural number k.

Properties of the congruence relation

- If $a \equiv b \pmod{m}$ and $d|m$, then $a \equiv b \pmod{d}$
- If $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, then $a \equiv b \pmod{lcm(m_1, m_2, \ldots, m_k)}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
- If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{m}$ for any integer k
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$
- If $a \equiv b \pmod{m}$, then $a + um \equiv b + vm \pmod{m}$ for every integers u and v
- If $ka \equiv kb \pmod{m}$ and $gcd(k, m) = 1$, then $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$ iff $ak \equiv bk \pmod{mk}$ for any natural number k.

Properties of the congruence relation

- If $a \equiv b \pmod{m}$ and $d|m$, then $a \equiv b \pmod{d}$
- If $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, then $a \equiv b \pmod{lcm(m_1, m_2, \ldots, m_k)}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
- If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{m}$ for any integer k
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$
- If $a \equiv b \pmod{m}$, then $a + um \equiv b + vm \pmod{m}$ for every integers u and v
- If $ka \equiv kb \pmod{m}$ and $gcd(k, m) = 1$, then $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$ iff $ak \equiv bk \pmod{mk}$ for any natural number k.

Properties of the congruence relation

- If $a \equiv b \pmod{m}$ and $d|m$, then $a \equiv b \pmod{d}$
- If $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, then $a \equiv b \pmod{lcm(m_1, m_2, \ldots, m_k)}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
- If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{m}$ for any integer k
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$
- If $a \equiv b \pmod{m}$, then $a + um \equiv b + vm \pmod{m}$ for every integers u and v
- If $ka \equiv kb \pmod{m}$ and $gcd(k, m) = 1$, then $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$ iff $ak \equiv bk \pmod{mk}$ for any natural number k.

Properties of the congruence relation

- If $a \equiv b \pmod{m}$ and $d|m$, then $a \equiv b \pmod{d}$
- If $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, then $a \equiv b \pmod{lcm(m_1, m_2, \ldots, m_k)}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
- If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{m}$ for any integer k
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$
- If $a \equiv b \pmod{m}$, then $a + um \equiv b + vm \pmod{m}$ for every integers u and v
- If $ka \equiv kb \pmod{m}$ and $gcd(k, m) = 1$, then $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$ iff $ak \equiv bk \pmod{mk}$ for any natural number k.

Properties of the congruence relation

- If $a \equiv b \pmod{m}$ and $d|m$, then $a \equiv b \pmod{d}$
- If $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, then $a \equiv b \pmod{lcm(m_1, m_2, \ldots, m_k)}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
- If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{m}$ for any integer k
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$
- If $a \equiv b \pmod{m}$, then $a + um \equiv b + vm \pmod{m}$ for every integers u and v
- If $ka \equiv kb \pmod{m}$ and $gcd(k, m) = 1$, then $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$ iff $ak \equiv bk \pmod{mk}$ for any natural number k.

Properties of the congruence relation

- If $a \equiv b \pmod{m}$ and $d|m$, then $a \equiv b \pmod{d}$
- If $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, then $a \equiv b \pmod{lcm(m_1, m_2, \ldots, m_k)}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
- If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{m}$ for any integer k
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$
- If $a \equiv b \pmod{m}$, then $a + um \equiv b + vm \pmod{m}$ for every integers u and v
- If $ka \equiv kb \pmod{m}$ and $gcd(k, m) = 1$, then $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$ iff $ak \equiv bk \pmod{mk}$ for any natural number k.

Properties of the congruence relation

- If $a \equiv b \pmod{m}$ and $d|m$, then $a \equiv b \pmod{d}$
- If $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, then $a \equiv b \pmod{lcm(m_1, m_2, \ldots, m_k)}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
- If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{m}$ for any integer k
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$
- If $a \equiv b \pmod{m}$, then $a + um \equiv b + vm \pmod{m}$ for every integers u and v
- If $ka \equiv kb \pmod{m}$ and $gcd(k,m) = 1$, then $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$ iff $ak \equiv bk \pmod{mk}$ for any natural number k.

Properties of the congruence relation

- If $a \equiv b \pmod{m}$ and $d|m$, then $a \equiv b \pmod{d}$
- If $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, then $a \equiv b \pmod{lcm(m_1, m_2, \ldots, m_k)}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
- If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{m}$ for any integer k
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$
- If $a \equiv b \pmod{m}$, then $a + um \equiv b + vm \pmod{m}$ for every integers u and v
- If $ka \equiv kb \pmod{m}$ and $gcd(k, m) = 1$, then $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$ iff $ak \equiv bk \pmod{mk}$ for any natural number k.

Warmup: An impossible Josephus problem

The problem

Ten people are sitting in circle, and every mth person is executed.
Prove that, for every $k \geqslant 1$, the first, second, and third person executed *cannot* be 10, k, and $k+1$, in this order.

Warmup: An impossible Josephus problem

The problem

Ten people are sitting in circle, and every mth person is executed.
Prove that, for every $k \geqslant 1$, the first, second, and third person executed *cannot* be 10, k, and $k+1$, in this order.

Solution

- If 10 is the first to be executed, then $10|m$.
- If k is the second to be executed, then $m \equiv k \pmod 9$.
- If $k+1$ is the third to be executed, then $m \equiv 1 \pmod 8$, because $k+1$ is the first one after k.

But if $10|m$, then m is even, and if $m \equiv 1 \pmod 8$, then m is odd: it cannot be both at the same time.

Application of congruence relation

Example 1: Find the remainder of the division of $a = 1395^4 \cdot 675^3 + 12 \cdot 17 \cdot 22$ by 7.

As $1395 \equiv 2 \pmod 7$, $675 \equiv 3 \pmod 7$, $12 \equiv 5 \pmod 7$, $17 \equiv 3 \pmod 7$ and $22 \equiv 1 \pmod 7$, then

$$a \equiv 2^4 \cdot 3^3 + 5 \cdot 3 \cdot 1 \pmod 7$$

As $2^4 = 16 \equiv 2 \pmod 7$, $3^3 = 27 \equiv 6 \pmod 7$, and $5 \cdot 3 \cdot 1 = 15 \equiv 1 \pmod 7$ it follows

$$a \equiv 2 \cdot 6 + 1 = 13 \equiv 6 \pmod 7$$

Application of congruence relation

Example 2: Find the remainder of the division of $a = 53 \cdot 47 \cdot 51 \cdot 43$ by 56.

A. As $53 \cdot 47 = 2491 \equiv 27 \pmod{56}$ and $51 \cdot 43 = 2193 \equiv 9 \pmod{56}$, then

$$a \equiv 27 \cdot 9 = 243 \equiv 19 \pmod{56}$$

B. As $53 \equiv -3 \pmod{56}$, $47 \equiv -9 \pmod{56}$, $51 \equiv -5 \pmod{56}$ and $43 \equiv -13 \pmod{56}$, then

$$a \equiv (-3) \cdot (-9) \cdot (-5) \cdot (-13) = 1755 \equiv 19 \pmod{56}$$

Application of congruence relation

Example 3: Find a remainder of dividing 45^{69} by 89

Make use of so called *method of squares*:

$$\begin{aligned}
45 &\equiv 45 \pmod{89} \\
45^2 = 2025 &\equiv 67 \pmod{89} \\
45^4 = (45^2)^2 \equiv 67^2 = 4489 &\equiv 39 \pmod{89} \\
45^8 = (45^4)^2 \equiv 39^2 = 1521 &\equiv 8 \pmod{89} \\
45^{16} = (45^8)^2 \equiv 8^2 = 64 &\equiv 64 \pmod{89} \\
45^{32} = (45^{16})^2 \equiv 64^2 = 4096 &\equiv 2 \pmod{89} \\
45^{64} = (45^{32})^2 \equiv 2^2 = 4 &\equiv 4 \pmod{89}
\end{aligned}$$

As $69 = 64 + 4 + 1$, then

$$45^{69} = 45^{64} \cdot 45^4 \cdot 45^1 \equiv 4 \cdot 39 \cdot 45 \equiv 7020 \equiv 78 \pmod{89}$$

Application of congruence relation

Let $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0$, where $a_i \in \{0, 1, \ldots, 9\}$ are digits of its decimal representation.

Theorem: An integer n is divisible by 11 iff the difference of the sums of the odd numbered digits and the even numbered digits is divisible by 11 :

$$11 | (a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots)$$

Proof.

Note, that $10 \equiv -1 \pmod{11}$. Then $10^i \equiv (-1)^i \pmod{11}$ for any i. Hence,

$$\begin{aligned} n &\equiv a_k(-1)^k + a_{k-1}(-1)^{k-1} + \ldots - a_1 + a_0 = \\ &= (a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots) \pmod{11} \end{aligned}$$

Q.E.D.

Example 4: 34425730438 is divisible by 11

Indeed, due to the following expression is divisible by 11:

$$(8 + 4 + 3 + 5 + 4 + 3) - (3 + 0 + 7 + 2 + 4) = 27 - 16 = 11$$

Next section

For determining whether a number n is prime.

There are alternatives:

- Try all numbers $2, \ldots, n-1$. If n is not dividisble by none of them, then it is prime.
- Same as above, only try numbers $2, \ldots, \sqrt{n}$.
- Probabilistic algorithms with polynomial complexity (the Fermat' test, the Miller-Rabin test, etc.).
- Deterministic primality-proving algorithm by Agrawal–Kayal–Saxena (2002).

For determining whether a number n is prime.

There are alternatives:

- Try all numbers $2, \ldots, n-1$. If n is not dividisble by none of them, then it is prime.
- Same as above, only try numbers $2, \ldots, \sqrt{n}$.
- Probabilistic algorithms with polynomial complexity (the Fermat' test, the Miller-Rabin test, etc.).
- Deterministic primality-proving algorithm by Agrawal–Kayal–Saxena (2002).

For determining whether a number n is prime.

There are alternatives:

- Try all numbers $2, \ldots, n-1$. If n is not dividisble by none of them, then it is prime.
- Same as above, only try numbers $2, \ldots, \sqrt{n}$.
- Probabilistic algorithms with polynomial complexity (the Fermat' test, the Miller-Rabin test, etc.).
- Deterministic primality-proving algorithm by Agrawal–Kayal–Saxena (2002).

For determining whether a number n is prime.

There are alternatives:

- Try all numbers $2, \ldots, n-1$. If n is not dividisble by none of them, then it is prime.
- Same as above, only try numbers $2, \ldots, \sqrt{n}$.
- Probabilistic algorithms with polynomial complexity (the Fermat' test, the Miller-Rabin test, etc.).
- Deterministic primality-proving algorithm by Agrawal–Kayal–Saxena (2002).

Next subsection

Fermat's "Little" Theorem

Theorem

If p is prime and a is an integer not divisible by p, then

$$p | a^{p-1} - 1$$

Lemma

If p is prime and $0 < k < p$, then $p | \binom{p}{k}$

Proof. This follows from the equality

$$\binom{p}{k} = \frac{p^{\underline{k}}}{k!} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1}$$

Pierre de Fermat

(1601–1665)

Another formulation of the theorem

Fermat's "little" theorem

If p is prime, and a is an integer, then $p|a^p - a$.

Proof.

- If a is not divisible by p, then $p|a^{p-1} - 1$ iff $p|(a^{p-1} - 1)a$
- The assertion is trivally true if $a = 0$. To prove it for $a > 0$ by induction, set $a = b + 1$. Hence,

$$
\begin{aligned}
a^p - a = (b+1)^p - (b+1) = \\
&= \binom{p}{0} b^p + \binom{p}{1} b^{p-1} + \cdots + \binom{p}{p-1} b + \binom{p}{p} - b - 1 = \\
&= (b^p - b) + \binom{p}{1} b^{p-1} + \cdots + \binom{p}{p-1} b
\end{aligned}
$$

Here the expression $(b^p - b)$ is divisible by p by the induction hypothesis, while other terms are divisible by p by the Lemma. Q.E.D.

Application of the Fermat' theorem

Example: Find a remainder of division the integer 3^{4565} by 13.

Fermat' theorem gives $3^{12} \equiv 1 \pmod{13}$. Let's divide 4565 by 12 and compute the remainder: $4565 = 380 \cdot 12 + 5$. Then

$$3^{4565} = (3^{12})^{380} 3^5 \equiv 1^{380} 3^5 = 81 \cdot 3 \equiv 3 \cdot 3 = 9 \pmod{13}$$

Application of the Fermat' theorem (2)

Prove that $n^{18}+n^{17}-n^2-n$ is divisible by 51 for any positive integer n.

Let's factorize

$$
\begin{aligned}
A = n^{18}+n^{17}-n^2-n = & \\
= n(n^{17}-n)+n^{17}-n = & \\
= (n+1)(n^{17}-n) = & \qquad \text{% From Fermat' theorem } \Rightarrow 17|A \\
= (n+1)n(n^{16}-1) = & \\
= (n+1)n(n^8-1)(n^8+1) = & \\
= (n+1)n(n^4-1)(n^4+1)(n^8+1) = & \\
= (n+1)n(n^2-1)(n^2+1)(n^4+1)(n^8+1) = & \\
= \underbrace{(n+1)n(n-1)}_{\text{divisible by 3}}(n+1)(n^2+1)(n^4+1)(n^8+1) &
\end{aligned}
$$

Hence, A is divisible by $17 \cdot 3 = 51$.

Next subsection

Fermat' test

Fermat' theorem: If p is prime and integer a is such that $1 \leqslant a < p$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

To test, whether n is prime or composite number:

- Check validity of $a^{n-1} \equiv 1 \pmod{n}$ for every $a = 2, 3, \ldots, n-1$.
- If the condtion is not satisfiable for one or more value of a, then n is composite, otherwise prime.

Example: is 221 prime?

$$\begin{aligned} 2^{220} &= \left(2^{11}\right)^{20} \equiv 59^{20} = \left(59^{4}\right)^{5} \equiv 152^{5} = \\ &= 152 \cdot \left(152^{2}\right)^{2} \equiv 152 \cdot 120^{2} \equiv 152 \cdot 35 = 5320 \equiv 16 \pmod{221} \end{aligned}$$

Hence, 221 is a composite number. Indeed, $221 = 13 \cdot 17$

Fermat' test

Fermat' theorem: If p is prime and integer a is such that $1 \leqslant a < p$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

To test, whether n is prime or composite number:

- Check validity of $a^{n-1} \equiv 1 \pmod{n}$ for every $a = 2, 3, \dots, n-1$.
- If the condtion is not satisfiable for one or more value of a, then n is composite, otherwise prime.

Example: is 221 prime?

$$\begin{aligned} 2^{220} &= \left(2^{11}\right)^{20} \equiv 59^{20} = \left(59^4\right)^5 \equiv 152^5 = \\ &= 152 \cdot \left(152^2\right)^2 \equiv 152 \cdot 120^2 \equiv 152 \cdot 35 = 5320 \equiv 16 \pmod{221} \end{aligned}$$

Hence, 221 is a composite number. Indeed, $221 = 13 \cdot 17$

Next section

Euler's totient function ϕ

Euler's totient function

Euler's totient function ϕ is defined for $m \geqslant 2$ as

$$\phi(m) = |\{n \in \{0, \ldots, m-1\} \mid gcd(m, n) = 1\}|$$

n	2	3	4	5	6	7	8	9	10	11	12	13
$\phi(n)$	1	2	2	4	2	6	4	6	4	10	4	12

টোশিয়েন্ট ফাংশনকে $\varphi(n)$ দিয়ে প্রকাশ করা হয়। $\varphi(n) = x$ যদি হয় তার মানে হচ্ছে 1 থেকে n পর্যন্ত x টা সংখ্যা আছে যাদের সাথে n এর GCD হচ্ছে 1। যদি $gcd(a, b) = 1$ হয় আমরা বলি a আর b কো-প্রাইম (co-prime)।

যেমন ধরো $n = 9$ এর জন্য $gcd(9, 3) = gcd(9, 6) = 3$ আর $gcd(9, 9) = 9$ আর বাকি ছটা সংখ্যার জন্য $gcd(9, 1) = gcd(9, 2) = gcd(9, 4) = gcd(9, 5) = gcd(9, 7) = gcd(9, 8) = 1$। সেজন্য, $\varphi(9) = 6$।

অয়লারের প্রোডাক্ট ফরমুলা অনুযায়ী টোশিয়েন্ট এর মান এভাবে বের করা যায় -

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

এখানে p হচ্ছে মৌলিক সংখ্যা আর $p|n$ মানে হচ্ছে সেইসব মৌলিক সংখ্যা যারা n কে নি:শেষে ভাগ করতে পারে। যেমন ধরো যখন আমরা লিখি $a|b$, এর মানে হচ্ছে a নি:শেষে ভাগ করতে পারে b কে। মানে, a হচ্ছে b এর ডিভিজর।

$$\begin{aligned}
\varphi(9) &= 9\prod_{p|n}(1-\frac{1}{p}) \\
&= 9(1-\frac{1}{3}) \\
&= 9\times\frac{2}{3} \\
&= 3\times 2 = 6
\end{aligned}$$

যেহেতু, $120 = 2^3\times 3^1\times 5^1$

$$\begin{aligned}
\varphi(120) &= 120\prod_{p|n}(1-\frac{1}{p}) \\
&= 120(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) \\
&= 120\times\frac{1}{2}\times\frac{2}{3}\times\frac{4}{5} \\
&= \frac{120\times 4}{15} \\
&= 8\times 4 \\
&= 32
\end{aligned}$$