

1. Let m_1 and m_2 are relatively prime positive integers, show that if $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$, then $a \equiv b \pmod{m_1 m_2}$.

Solution: Since $a \equiv b \pmod{m_1}$, we have $m_1 | (a - b)$. Similarly we have $m_2 | (a - b)$. Because m_1 and m_2 are relatively prime positive integers, we know both m_1 and m_2 are different factors of $a - b$. We can conclude that $m_1 m_2 | (a - b)$. That is to say $a \equiv b \pmod{m_1 m_2}$.

2. Use Fermat's Little theorem to compute $3^{302} \pmod{5}$

Solution: From Fermat's Little theorem, we have $3^{5-1} \equiv 1 \pmod{5}$. So $3^{302} = 3^{4 \times 75 + 2} = (3^4)^{75} \times 3^2 \equiv (3^4)^{75} \pmod{5} \times 3^2 \pmod{5} = 1 \times 4 = 4$.

3. Show that if a and b are positive integers, then $(2^a - 1) \pmod{(2^b - 1)} = 2^{a \pmod{b}} - 1$.

Solution: Let $a = k b + r$ and $r = a \pmod{b}$, then $(2^a - 1) - (2^{a \pmod{b}} - 1) = 2^{k b + r} - 2^r = 2^r(2^{k b} - 1) = 2^r(2^b - 1)(2^{b(k-1)} + \dots + 1) = (2^b - 1)(2^r(2^{b(k-1)} + \dots + 1))$. Therefore, $(2^a - 1) \pmod{(2^b - 1)} = 2^{a \pmod{b}} - 1$.

1.

4. Find the inverse of 2 (mod 100).

Solution: This is a tricky question. No solution exists for this question because $\gcd(2, 100) = 2$. not 1.

5. Find the inverse of 3 (mod 20).

Solution: First, you need to apply the Euclidean algorithm until you get a remainder 1. Then you should do back-substitution. Of course, you can use the Extended Euclidean algorithm to solve this problem.

Use Euclidean algorithm (Top Down)

$$20 = 3 \times 6 + 2$$

$$3 = 2 \times 1 + 1$$

now we get the remainder 1. We use back-substitution to get $1 = s a + t b$. (Bottom Up)

$$1 = 3 - 2 \times 1 = 3 - (20 - 3 \times 6) = -20 + 7 \times 3 = (-1) \times 20 + 7 \times 3$$

Therefore, $7 \times 3 \equiv 1 \pmod{20}$. The solution is 7.

6. Show that if m is a positive integer greater than 1 and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m/\gcd(c, m)}$.

Solution: From $ac \equiv bc \pmod{m}$, we know \exists integer k such that $ac - bc = mk$. Let $g = \gcd(c, m)$ and divide g we get $(a - b)(c/g) = (m/g)k$. Since $\gcd(c/g, m/g) = 1$, we know $(c/g) \mid k$. Divide c/g on both sides, we get $a - b = (m/g) \times \frac{k}{c/g}$. Therefore, we know $a \equiv b \pmod{m/\gcd(c, m)}$.