Consistency of equations

Any system of equations

$$x \equiv b_1 \bmod n_1$$
$$\vdots$$
$$x \equiv b_r \bmod n_r$$

where n_i and n_j are coprime for $i \neq j$ has a unique solution mod $\prod n_i$;

because then $\operatorname{lcm}(n_1 \dots n_r) = n_1 \times \dots \times n_r = \prod_{i=1}^{r} n_i = n$

and $b \bmod n \longmapsto (b \bmod n_1, \dots, b \bmod n_r)$ is a bijection. In other cases we might need to work to see if the equations are consistent, that is, if they have a solution.

Examples $\left.\begin{aligned} x &\equiv 1 \bmod 21 \\ x &\equiv 2 \bmod 9 \end{aligned}\right\} \Longrightarrow \begin{aligned} x &\equiv 1 \bmod 3,\ x \equiv 1 \bmod 7 \\ x &\equiv 2 \bmod 3,\ x \equiv 2 \bmod 9 \end{aligned}$

So is consistent.

$$\left.\begin{aligned} 3x &\equiv 6 \bmod 21 \\ x &\equiv 2 \bmod 9 \end{aligned}\right\} \begin{aligned} &\Longleftrightarrow x \equiv 2 \bmod 7 \\ &\Longrightarrow x \equiv 2 \bmod 9 \end{aligned}$$

has a solution $(x \equiv 2 \bmod 63)$

$$\left.\begin{aligned} 14x &\equiv 7 \bmod 21 \\ x &\equiv 2 \bmod 9 \end{aligned}\right\} \Longleftrightarrow \begin{aligned} 2x &\equiv 1 \bmod 3 \Longleftrightarrow x \equiv 2 \bmod 3. \\ x &\equiv 2 \bmod 9 \end{aligned}$$

Solution is $x \equiv 2 \bmod 9$!

Chinese Remainder Theorem

This is the theorem that if $\gcd(n_i, n_j) = 1 \quad \forall i \neq j$

then $x \equiv a_i \mod n_i \quad (1 \leq i \leq r)$

has a unique solution mod n where $n = \prod_{i=1}^{r} n_i$

The Chinese proof is a formula that is very useful.

$$x \equiv a_i \mod n_i \iff$$

$$x = a_1\left(\left(\prod_{j\neq 1} n_j\right)^{-1} \mod n_1\right)\left(\prod_{j\neq 1} n_j\right) + \cdots + a_r\left(\left(\prod_{j\neq r} n_j\right)^{-1} \mod n_r\right)\prod_{j\neq r} n_j \mod n.$$

n_i divides all the terms in the sum apart from the i^{th}.

Examples

Solve $79x \equiv 1 \mod 90$

This can of course be done using the Euclidean algorithm to compute $79^{-1} \mod 90$.

Alternatively this is equivalent to

$$79x \equiv 1 \mod 5$$
$$79x \equiv 1 \mod 2$$
$$79x \equiv 1 \mod 9$$

$4x \equiv 1 \mod 5, \quad x \equiv 1 \mod 2, \quad 7x \equiv 1 \mod 9$

$\Leftrightarrow x \equiv 4 \mod 5, \quad x \equiv 1 \mod 2, \quad x \equiv 4 \mod 9$

$\Leftrightarrow \quad x \equiv 4 \bmod 45 \qquad x \equiv 1 \bmod 2$

$\gcd(45,1) = 1$

$x = 4 \times (2^{-1} \bmod 45) \times 2 + 1 \times (45^{-1} \bmod 2) \times 45 \bmod 90$

$= 4 \times 23 \times 2 + 1 \times 1 \times 45 \bmod 90$

$= 4 \times 46 + 45 \bmod 90 \equiv 4 + 45 \equiv 49 \bmod 90$

Clearly satisfies $49 \equiv 4 \bmod 45$ and $\equiv 1 \bmod 2$.

Check $79 \times 49 = 3871 = (43 \times 90) + 1 \equiv 1 \bmod 90$

Using the Euclidean algorithm

$$\left(\begin{array}{cc|c} 1 & 0 & 90 \\ 0 & 1 & 79 \end{array}\right) \xrightarrow{R_1 - R_2} \left(\begin{array}{cc|c} 1 & -1 & 11 \\ 0 & 1 & 79 \end{array}\right) \xrightarrow[R_2 - 7R_1]{} \left(\begin{array}{cc|c} 1 & -1 & 11 \\ -7 & 8 & 2 \end{array}\right)$$

$$\xrightarrow{R_1 - 5R_2} \left(\begin{array}{cc|c} 36 & -41 & 1 \\ -7 & 8 & 2 \end{array}\right)$$

$36 \times 90 - 41 \times 79 = 1$

$79 \times (-41) \equiv 1 \bmod 90$

This agrees with the previous answer as

$-41 \equiv 49 \bmod 90.$

Other examples

② $x \equiv 3 \bmod 5$

$x \equiv 2 \bmod 7$

$x \equiv 1 \bmod 11$

$x \equiv 3 \times (77^{-1} \bmod 5) \times 77 + 2 \times (55^{-1} \bmod 7) \times 55 + 1 \times (35^{-1} \bmod 11) \times 35 \bmod 385$

$\equiv 3 \times (2^{-1} \bmod 5) \times 77 + 2 \times (6^{-1} \bmod 7) \times 55 + 1 \times (2^{-1} \bmod 11) \times 35$

$\equiv 9 \times 77 + 12 \times 55 + 6 \times 35$

$\equiv (-1) \times 77 + 5 \times 55 - 5 \times 35 \bmod 385$

$\equiv -77 + 100 \equiv 23 \bmod 385$

③ $2x \equiv 1 \bmod 5 \Rightarrow x \equiv 3 \bmod 5$

$3x \equiv 2 \bmod 7 \Rightarrow x \equiv 3 \bmod 7$ (mult by 5)

$x \equiv 1 \bmod 3$

So $x \equiv 3 \bmod 35$, $x \equiv 1 \bmod 3$

$x \equiv 3 \times (3^{-1} \bmod 35) \times 3 + 1 \times (35^{-1} \bmod 3) \times 35 \bmod 105$

$\equiv 3 \times 12 \times 3 + 1 \times 2^{-1} \bmod 3 \times 35 \bmod 105$

$= 3 \times 36 + 70 \bmod 105$

$\equiv 178 \equiv 73 \bmod 105$

(4)

(i) $2x \equiv 4 \bmod 6 \iff x \equiv 2 \bmod 3$

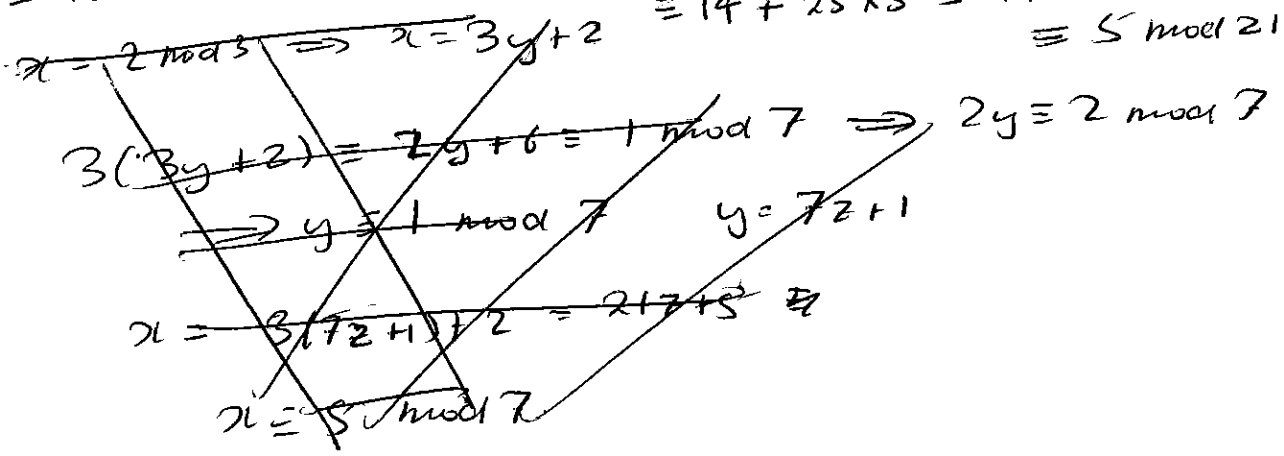
(ii) $3x \equiv 1 \bmod 7 \iff x \equiv 5 \bmod 7$

$x \equiv 2 \times (7^{-1} \bmod 3) \times 7 + 5 \times (3^{-1} \bmod 7) \times 3 \bmod 21$

$\equiv 14 + 25 \times 3 \equiv 14 + 12 \bmod 21$

$\equiv 5 \bmod 21$

1a (ii)



(5)

$3x \equiv 2 \bmod 5 \Rightarrow x \equiv 2 \times 3x \equiv 4 \bmod 5$

$3x \equiv 6 \bmod 17 \Rightarrow x \equiv 2 \bmod 17$

Using the Chinese Remainder Theorem

$x \equiv 4 \times (17^{-1} \bmod 5) \times 17 + 2 \times (5^{-1} \bmod 17) \times 5$

$\equiv 4 \times (2^{-1} \bmod 5) \times 17 + 2 \times 7 \times 5$

$\equiv 4 \times 3 \times 17 + 70 \equiv 12 \times 17 + 70 \bmod 85$

$\equiv 2 \times 17 - 15 \equiv 19 \bmod 85$

(6) $3x \equiv 4 \bmod 11$ $2x \equiv 6 \bmod 7$ $3x \equiv 2 \bmod 5$

$4 \times 3x \equiv x \equiv 16 \equiv 5 \bmod 11$ $x \equiv 3 \bmod 7$ $2 \times 3x \equiv x \equiv 4 \bmod 5$

Using the Chinese Remainder Theorem

$x \equiv 5 \times (35^{-1} \bmod 11) \times 35 + 3 \times (55^{-1} \bmod 7) \times 55 + 4 \times (77^{-1} \bmod 5) \times 77$

$\equiv 5 \times (2^{-1} \bmod 11 \times 35) + 3 \times ((-1)^{-1} \bmod 7) \times 55 + 4 \times (2^{-1} \bmod 5) \times 77$

$\equiv 5 \times 6 \times 35 - 3 \times 55 + 4 \times 3 \times 77 \bmod 77 \times 5 = 385$

$\equiv 3 \times 350 - 3 \times 55 + 12 \times 77 \bmod 385$

$\equiv 3 \times 295 + 2 \times 77 \equiv 885 + 154 \equiv 115 + 154 \equiv 269 \bmod 385$

(7) So Find all solutions to

$4x \equiv 5 \bmod 9$ $\quad 2x \equiv 6 \bmod 12$ $\quad 3x \equiv 4 \bmod 7$

Equivalently $7 \times 4x \equiv x \equiv 8 \bmod 9$ $\quad x \equiv 3 \bmod 6$ $\quad 5 \times 3x \equiv x \equiv 6 \bmod 7$

$x \equiv 8 \bmod 9 \Rightarrow x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 6 \Rightarrow x \equiv 0 \bmod 3$

So there are no solutions.

(8) A nonlinear example.

Find all solutions to $x^2 \equiv x \bmod 100$

$x(x-1) \equiv 0 \bmod 100 \Rightarrow 100 \mid x(x-1) \Rightarrow 2^2 \times 5^2 \mid x(x-1)$

If $2 \mid x$ then $2 \nmid x-1$ and if $2 \mid x-1$ then $2 \nmid x$ because $2 \nmid 1$

So either $2^2 \mid x$ or $2^2 \mid x-1$

Similarly either $5^2 \mid x$ or $5^2 \mid x-1$

If $2^2 \mid x$ and $5^2 \mid x$ then $100 \mid x$ and $x \equiv 0 \bmod 100$

If $2^2 \mid x-1$ and $5^2 \mid x-1$ then $100 \mid x-1$ and $x \equiv 1 \bmod 100$

If $2^2 \mid x$ and $5^2 \mid x-1$ then by considering $1, 26, 51, 76$

we see that $x \equiv 76 \bmod 100$

If $2^2 \mid x-1$ and $5^2 \mid x$ then from considering $0, 25, 50, 75$

we see that $x \equiv 25 \bmod 100$

So altogether $x \equiv 0, 1, 25$ or $76 \bmod 100$

Use the order of an element mod n

We have seen that for any $n \in \mathbb{Z}_+$, $n \geq 2$

$G_n = \{ m \bmod n : \gcd(m,n) = 1 \}$ is a group under multiplication.

If n is prime then $G_n = \{ m \bmod n : 1 \leq m < n \}$

Def^n If G is any finite group then the order of $g \in G$ is the smallest integer m s.t. $g^m = 1$

Examples in $G_3 = \{1, 2\}$ the order of 1 is 1 and 2 is 2

$1^1 = 1$ $2^1 \not\equiv 1 \bmod 3$ $2^2 \equiv 1 \bmod 3$

$G_4 = \{1, 3\}$. $3^2 \equiv 1 \bmod 4$. The order of 3 is 2

$G_5 = \{1, 2, 3, 4\}$ $2^2 = 4$ $2^3 \equiv 3 \bmod 5$ $2^4 \equiv 1$

$3^2 \equiv 4$ $3^3 \equiv 2$ $3^4 \equiv 1$

The orders of 2 and 3 are 4 (mod 5)

The order of 4 is 2 mod 5 because $4^2 \equiv 1 \bmod 5$

Fermat's Little Theorem

If p is prime and $\gcd(a,p) = 1$ then

$a^{p-1} \equiv 1 \bmod p$

For all integers a, $a^p \equiv a \bmod p$

Euler's Theorem

If $n \geq 2$ is any integer and a is coprime to n,

$a^{\phi(n)} \equiv 1 \bmod n$.

This is a generalisation of the previous theorem because if p is prime then $\phi(p) = p - 1$

Proof of both these theorems

In a finite group G, the order of any element divides the order $|G|$ of the group. (This is in itself a special case of Lagrange's Theorem; that the order of any subgroup $\{g^i : i \geq 1\}$ divides $|G|$. In this case the subgroup is $\{g^i : i \geq 1\}$ whose order is the order of g.)

$|G_n| = \phi(n)$ so the order of any element of G_n divides $\phi(n)$ and $a^{\phi(n)} \equiv 1 \bmod n \ \forall a \in G_n$.

Examples (1) 17 is prime so $a^{16} \equiv 1 \bmod 17$ whenever $\gcd(a, 17) = 1$ e.g. $2^{16} \equiv 1 \bmod 17$

Check: $2^2 = 4$ $2^4 = 16 \equiv -1 \bmod 17$ so $2^8 \equiv (-1)^2 \equiv 1 \bmod 17$

So $2^{16} \equiv 1^2 \equiv 1 \bmod 17$.

$3^2 = 9$ $3^4 = 81 \equiv -4 \bmod 17$ $3^8 \equiv (-4)^2 \equiv 16 \equiv -1 \bmod 17$

$3^{16} \equiv (-1)^2 \equiv 1 \bmod 17$.

(2) $|G_{24}| = \phi(24) = \phi(8) \times \phi(3) = 2^2(2-1) \times (3-1) = 8$

$G_{24} = \{\pm 1, \pm 5, \pm 7 \pm 11\}$

$5^2 \equiv 1 \bmod 24$ $7^2 \equiv 1$, $11^2 = 121 \equiv 1 \bmod 24$

So $5^8 \equiv 7^8 \equiv 11^8 \equiv 1$.

(3) Show that $5^{50} + 3^{130}$ is divisible by 17

$5^{16} \equiv 1 \equiv 3^{16} \mod 17$ by Fermat's Little Theorem

$5^{50} \equiv 5^{48} \times 5^2 \equiv 5^2 \equiv 8 \mod 17$

$3^{130} \equiv 3^{128} \times 3^2 \equiv 3^2 \equiv 9 \mod 17$

So $5^{50} + 3^{130} \equiv 8 + 9 + 0 \mod 17$

Checking primality of $2^n - 1$

Recall that if $2^n - 1$ prime then n must be prime and these are the *Mersenne primes*

$2^n - 1$ is prime for $n = 2, 3, 5, 7, 13, 17, 19, 31 \ldots$ but not for $n = 11, 23, 29$

If p and n are prime

$p \mid 2^n - 1 \iff 2^n \equiv 1 \mod p \iff 2^{na + b(p-1)} \equiv 1 \mod p$

$\forall a, b \in \mathbb{Z}$ (by Fermat's Little Theorem, since $2^{p-1} \equiv 1 \mod p$)

$\Longrightarrow 2^g \equiv 1 \mod p$ where $g = \gcd(n, p-1)$

$2^1 \not\equiv 1 \mod p$ and n is prime, so $g = n$ and

$n \mid p-1$ that is $p \equiv 1 \mod n$.

So if p and n are prime, $p \mid 2^n - 1 \Rightarrow p \equiv 1 \mod n$.

Example $n = 11$

$p \mid 2^{11}-1 \iff 2^{11} \equiv 1 \bmod p \implies 11 \mid p-1 \implies p \equiv 1 \bmod 11.$

But $2^{11}-1$ odd $\implies p$ odd $\implies p \equiv 1 \bmod 2$

So $p \mid 2^{11}-1 \implies p \equiv 1 \bmod 22$

The first possibility is $p = 23$, and $2^{11}-1 = 2047 = 28 \times 89$.

$n = 13$

$p \mid 2^{13}-1 \iff 2^{13} \equiv 1 \bmod p \implies 13 \mid p-1 \implies p \equiv 1 \bmod 13$

$\implies p \equiv 1 \bmod 26$ (because p is odd)

$\sqrt{2^{13}-1} = 90.\ldots$ So if p exists with $p < 2^{13}-1$ then

p exists with $p < 90$ and $p \equiv 1 \bmod 26$

So $p = 53$ or 79. Neither of these works.

$n = 23$

$p \mid 2^{23}-1 \implies p \equiv 1 \bmod 23 \implies p \not\equiv 1 \bmod 46$

The first possibility is $p = 47$ and it turns out that $47 \mid 2^{23}-1$

$n = 29$

$p \mid 2^{29}-1 \implies p \equiv 1 \bmod 29 \implies p \equiv 1 \bmod 58$

The first possibilities are $p = 59$, $p = 233$, —

It turns out that $233 \mid 2^{29}-1$.

~~Examples~~

Fermat Pseudo primes.

Fermat's Little Theorem is the basis of a primality test. called Fermat's Primality Test.

If n is prime, then $a^{n-1} \equiv 1 \bmod n$ $\forall$ a coprime to n,

in particular for $1 \leq a < n$.

So if $\exists a$ with $1 \leq a < n$ and $a^{n-1} \not\equiv 1 \bmod n$, then we know that a is not prime ~~we then~~

Examples Using the Big Number Calculator,

(1) Let $n = 841$ $a \equiv 2$ $2^{840} \equiv 30$ So 841 is not prime. In fact $841 = 29 \times 29$.

So by Euler's Theorem $a^{\phi(841)} \equiv 1$ $\forall$ a coprime to 841, that is, coprime to 29. $\phi(841) = \phi(29^2) = 29 \times 4 \times 7$

(2) Let $n = 65431$, $2^{65430} \equiv 37824 \bmod 65431$

So 65431 is not prime. In fact, $65431 = 59 \times 1109$

(3) $n = 341$ $a = 2$ $2^{340} \equiv 1 \bmod 341$

Does this mean 341 is prime?

No, because if $a = 3$, $3^{340} \equiv 56 \bmod 341$.

So n is not prime n is a pseudo-prime to base 2

but 2 is a Fermat liar for 341

Definition n is a pseudoprime to base a if $1 \leq a < n$ and $a^{n-1} \equiv 1 \bmod n$ ~~but n is not prime~~

If in addition n is not prime, we say that a is a Fermat liar for n.

(4) $n = 2047 = 2^{11} - 1$

$2^{2046} \equiv 1 \bmod 2047$

$3^{2046} \equiv 1013 \bmod 2047.$

So 2047 is a pseudoprime to base 2 – but is not prime

2 is a Fermat liar for 2047.

Why? $2^{10} \equiv 1 \bmod 11$ by Fermat's Little Theorem

So $11 \mid 2^{10} - 1$ (Check: $2^{10} - 1 = 1023$)

So $11 \mid 2^{11} - 2 = n - 1$ $\quad 2^{11} \equiv 1 \bmod n.$

$11 \times k = (n-1)$ $\quad 2^{n-1} \equiv (2^{11})^k \equiv 1 \bmod n.$

For (3) : $341 = 11 \times 31$.

$2^{10} \equiv 1 \bmod 11$ by Fermat's Little Theorem

$2^{340} = (2^{10})^{34} \equiv 1 \bmod 11.$

$2^5 \equiv 1 \bmod 31$ because $2^5 = 32$

So $2^{340} \equiv (2^5)^{68} \equiv 1 \bmod 31.$ So $2^{340} \equiv 1 \bmod 31 \times 11.$