$u = 70,\ v = 21,\ w = 18$

$\gcd(70, 21, 18) = a \cdot 70 + b \cdot 21 + c \cdot 18$

$d_1 = \gcd(70, 21)$ $\qquad$ $d = \gcd(d_1, 18)$

$d_1 = \alpha \cdot 70 + \beta \cdot 21$ $\qquad$ $d = \gamma \cdot d_1 + \varepsilon \cdot 18$

$d = \gamma \cdot \alpha \cdot 70 + \gamma \cdot \beta \cdot 21 + \varepsilon \cdot 18$

1) Prove that $\hat{17} \in U(\mathbb{Z}_{54})$

2) Find the inverse of $\hat{17}$

3) $|U(\mathbb{Z}_{54})| = ?$

Sol 3)

54	2
27	3
9	3
3	3
1	

$54 = 2 \cdot 3^3$

$\varphi(54) = 54\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)$

$= 54 \cdot \frac{1}{2} \cdot \frac{2}{3} = 18$

Sol 2) $\gcd(17, 54) = 1$

$54 : 17 = 3$ rest 3 $\quad 54 = 17 \cdot 3 + 3$

$17 : 3 = 5$ rest 2 $\quad 17 = 3 \cdot 5 + 2$

$3 : 2 = 1$ rest 1 $\quad 3 = 2 \cdot 1 + \boxed{1}$

$2 : 1 = 2$ rest 0 $\quad 2 = 1 \cdot 2 + 0$

$\gcd(17, 54) = 1$

$17a + 54 \cdot v = 1 =$

$= 3 - 2 \cdot 1 = 3 - (17 - 3 \cdot 5)$

$= 3 - 17 + 3 \cdot 5 = 6 \cdot 3 - 17$

$= 6 \cdot (54 - 17 \cdot 3) - 17 =$

$= 6 \cdot 54 - 18 \cdot 17 - 17$

$= 6 \cdot 54 - 19 \cdot 17 = 1$

$\widehat{6 \cdot 54} - \widehat{19 \cdot 17} = \hat{1} \Leftrightarrow$

$\Leftrightarrow -\widehat{19} \cdot \widehat{17} = \hat{1}$

$\Leftrightarrow$ The inverse of $\hat{17}$ is $-\hat{19} = \widehat{54 - 19} = \hat{35}$

$\underbrace{6 \cdot 54}_{\equiv 0} - 19 \cdot 17 \overset{54}{\equiv} 1$

$0 - 19 \cdot 17 \overset{54}{\equiv} 1$

-19 is the inverse of 17

$\Rightarrow \hat{17}^{-1} = \widehat{-19} = \hat{35}$

Lol 1) Since $\gcd(17,54)=1 \Rightarrow \hat{17} \in U(\mathbb{Z}_{54})$

$\hat{a} \in \mathbb{Z}_n$

$\hat{a} \in U(\mathbb{Z}_n) \Leftrightarrow \gcd(a,n) = 1$

find one equivalent $u \cdot a + v \cdot n = 1$

$\Rightarrow \hat{u} \cdot \hat{a} + \hat{0} = \hat{1}$ in $\mathbb{Z}_n$

$\Rightarrow \hat{a}^{-1} = \hat{u}$

Prop

Let $n \geq 2$

T.F.A.E:

1) $\mathbb{Z}_n$ is a field
2) n is a prime
3) $\mathbb{Z}_n$ is a domain (or an integral ring) "inel integru"

(1), (2), (3) def.

i.e. $\forall \hat{a}, \hat{b} \in \mathbb{Z}_n \setminus \{\hat{0}\} \Rightarrow \hat{a} \cdot \hat{b} \neq \hat{0}$

i.e. $\mathbb{Z}_n$ has no nonzero divisors

i.e. $\forall \hat{a}, \hat{b} \in \mathbb{Z}_n$ s.t. $\hat{a} \cdot \hat{b} = \hat{0} \Rightarrow \hat{a} = \hat{0}$ or $b = \hat{0}$

(3) def.

$\mathbb{Z}_n$ field $\overset{\text{def}}{\iff} U(\mathbb{Z}_n) = \mathbb{Z}_n / \{0\}$

$\iff |U(\mathbb{Z}_n)| = n-1$ (because $\hat{0}$ is not invertible in $\mathbb{Z}_n$)

$\iff \varphi(n) = n-1$

$\iff$ all numbers $1 \leq x \leq n-1$; $\gcd(x, n) = 1$

$\iff n$ is prime

Say $\hat{a} \cdot \hat{b} = \hat{0}$ in $\mathbb{Z}_n$

$\widehat{ab} = \hat{0} \Leftrightarrow n \mid a \cdot b$

$\hat{a} = \hat{0} \iff n \mid a$

$\hat{b} = \hat{0} \iff n \mid b$

$n \mid a\,b \Rightarrow n \mid a$ or $n \mid b$

if and only if n is prime

Find the last 2 digits of $N = 181^{365}$

$= \ldots 01$

Find $n \bmod 100 = ?$

$$181^{365} \overset{100}{\equiv} (181 \bmod 100)^{365} \overset{100}{\equiv} 81^{365} \equiv (81^5)^{73} \overset{100}{\equiv} 1^{73} \bmod 100$$

$81^1 \equiv 81$

$81^2 \overset{100}{\equiv} (-19)^2 \overset{100}{\equiv} 19^2 \equiv 361 \equiv 61$

$81^3 \overset{100}{\equiv} 81 \cdot 61 \equiv 41$

$81^4 \overset{100}{\equiv} 61^2 \equiv 21^2$

$81^5 \overset{100}{\equiv} 1 \bmod 100$

Find the reminder $N = 131^{1111}$ when divided by 9

$$131^{1111} \overset{9}{\equiv} (131 \bmod 9)^{1111} \overset{9}{\equiv} 5^{1111}$$

$$5^1 \overset{9}{\equiv} 5$$
$$5^2 \overset{9}{\equiv} 25 \overset{9}{\equiv} 7$$
$$5^3 \overset{9}{\equiv} 125 \overset{9}{\equiv} 8 \quad \text{or} \quad 5^3 \overset{9}{\equiv} 5 \cdot 7 \overset{9}{\equiv} 35 \overset{9}{\equiv} 8$$
$$5^4 \overset{9}{\equiv} 5 \cdot 8 \overset{9}{\equiv} 40 \equiv 4$$
$$5^6 \overset{9}{\equiv} 5 \cdot 4 \overset{9}{\equiv} 2$$
$$5^6 \overset{9}{\equiv} 5 \cdot 2 \overset{9}{\equiv} 1$$

$$5^{1111} \equiv \left(5^6\right)^{185} \cdot 5 \equiv 1 \cdot 5 \equiv 5 \bmod 9$$

$$1111 = 6 \cdot 185 + 1$$

$$\hat{5} \in U(\mathbb{Z}_9)$$

Because $|U(\mathbb{Z}_9)| = 6 \rightarrow (U(\mathbb{Z}_9), \cdot)$ is a group with 6 elements

Lagrange's Thm $\Rightarrow$ $\hat{5}^6 \equiv \hat{1}$ in $\mathbb{Z}_9$

$$5^6 = 1 \bmod 9$$

Fermat's Theorem: If p prime $a \in \mathbb{Z}$ $p \nmid a$, then $a^{p-1} \equiv 1 \bmod p$

p prime $|U(\mathbb{Z}_p)| = p-1$, $\hat{a} \in U(\mathbb{Z}_p)$

Fermat's Primality Test

input: $n \in \mathbb{N}$, $n \geq 2$

output: is n a prime number?

1) Pick any $a \in \mathbb{N}$, $p \nmid a$
2) If $a^{n-1} \not\equiv 1 \bmod n$, then n is not prime
   If $a^{n-1} \equiv 1 \bmod n$, then GO TO STEP 1

If $a^{n-1} \not\equiv 1 \bmod n$ we say that

"a is a FERMAT WINTNESS for the primality of n"

In practice: one repeats $\simeq 10-12$ times

Def: The number $\in \mathbb{N}$ is called a CARMICHAEL number if it is a composite and it has no witness for the Fermat test

Exercise: Prove that $n = 561$ is a Carmichel number

$561 = 3 \cdot 11 \cdot 17$ not prime

Test: Any $a \in \mathbb{N}$ $\gcd(a, 561) = 1 \Rightarrow$

$\Rightarrow a^{560} \equiv 1 \mod 561$

$\varphi(561) = 561 \cdot \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{11}\right)\left(1 - \frac{1}{17}\right) = 2 \cdot 10 \cdot 16 = 320$

$$\gcd(a, 561) \Leftrightarrow \begin{cases} \gcd(a,3)=1 & \overset{\text{Fermat's}}{\longleftrightarrow} \quad a^2 \equiv 1 \bmod 3 \\ \gcd(a,11)=1 & \overset{\text{Thm}}{\longleftrightarrow} \quad a^{10} \equiv 1 \bmod 11 \\ \gcd(a,17)=1 & \longleftrightarrow \quad a^{16} \equiv 1 \bmod 16 \end{cases}$$

$$\Rightarrow a^{560} = (a^2)^{280} = 1^{280} = 1 \bmod 3$$

$$\Rightarrow a^{560} = (a^{10})^{56} \equiv 1 \bmod 11$$

$$\Rightarrow a^{560} = (a^{16})^{35} = 1 \bmod 17$$

$$\Rightarrow 3 \mid a^{560} - 1$$

$$\& \; 11 \mid a^{560} - 1 \quad \Rightarrow 3 \cdot 11 \cdot 17 \mid a^{560} - 1$$

$$\& \; 17 \mid a^{560} - 1$$

$$\Rightarrow a^{560} \equiv 1 \bmod 561$$

So 561 is a composite number number, but it has no Fermat witneses.