Homework 4

250H Spr 2024

Show that if $x \equiv 0 \pmod{21}$ and $y \equiv 0 \pmod{24}$ then $x+y \equiv 0 \pmod{3}$.

Proof: Let $x \equiv 0 \pmod{21}$ and $y \equiv 0 \pmod{24}$. Then by definition, $x = 21k$ and $y = 24j$ for $k, j \in \mathbf{Z}$. So,

$$x + y = 21k + 24j$$

$$= 3(7k + 8j)$$

Since, $7k + 8j \in Z$, $x + y \equiv 0 \pmod{3}$. ☽

Make a conjecture and prove it of the form If $x \equiv 0 \pmod{m}$ and $y \equiv 0 \pmod{n}$ then $x+y \equiv 0$ (mod BLANK)

In order, for $x+y \equiv 0$ (mod BLANK), we need BLANK to be a factor of both x and y. To simplify our proof, let us say that BLANK is the gcd(x,y).

Def of GCD: Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b.

Proof: Let $x \equiv 0 \pmod{m}$, $y \equiv 0 \pmod{n}$, and $\gcd(m, n) = d$ for $m, n, d \in \mathbb{Z}$. Then by definition, $d \mid x$ and $d \mid y$. So, $x = dk$ and $y = dj$ for $k, j \in \mathbb{Z}$. So,

$$x + y = dk + dj$$

$$= d(k + j)$$

Since, $k + j \in Z$, $x + y \equiv 0 \pmod{d} \equiv 0 \pmod{\gcd(m,n)}$. ☽

Compute the following MOD 23 and spot a pattern 7^0 , 7^1 , 7^2 , . . . Give us that pattern.

$7^0 = 1$	$7^5 = 17$	$7^{10} = 13$	$7^{15} = 14$	$7^{20} = 8$
$7^1 = 7$	$7^6 = 4$	$7^{11} = 22$	$7^{16} = 6$	$7^{21} = 10$
$7^2 = 3$	$7^7 = 5$	$7^{12} = 16$	$7^{17} = 19$	$7^{22} = 1$
$7^3 = 21$	$7^8 = 12$	$7^{13} = 20$	$7^{18} = 18$	$7^{23} = 7$
$7^4 = 9$	$7^9 = 15$	$7^{14} = 2$	$7^{19} = 11$	$7^{24} = 3$

Pattern: $7^n \equiv 7^{n+a} \equiv 7^{n+2a} \equiv \ldots$

a = 22

Use that pattern to compute 7^{1000} (mod 23)

$7^0 = 1$	$7^5 = 17$	$7^{10} = 13$	$7^{15} = 14$	$7^{20} = 8$
$7^1 = 7$	$7^6 = 4$	$7^{11} = 22$	$7^{16} = 6$	$7^{21} = 10$
$7^2 = 3$	$7^7 = 5$	$7^{12} = 16$	$7^{17} = 19$	$7^{22} = 1$
$7^3 = 21$	$7^8 = 12$	$7^{13} = 20$	$7^{18} = 18$	$7^{23} = 7$
$7^4 = 9$	$7^9 = 15$	$7^{14} = 2$	$7^{19} = 11$	$7^{24} = 3$

$7^{1000} = 7^{10 + 22(45)}$

$\equiv 7^{10} \equiv 13 \pmod{23}$

7^{1000} (mod 23) using in class method

- Write 1000 as a sum of powers of 2.
  - $2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^3$
- Fill in the following table:
  - $7^{2\text{^}0} \equiv 1 \pmod{23}$
  - $7^{2\text{^}1} \equiv (7^{2\text{^}0})^2 \equiv 7^2 \equiv 3 \pmod{23}$
  - $7^{2\text{^}2} \equiv (7^{2\text{^}1})^2 \equiv 3^2 \equiv 9 \pmod{23}$
  - $7^{2\text{^}3} \equiv (7^{2\text{^}2})^2 \equiv 9^2 \equiv 12 \pmod{23}$
  - $7^{2\text{^}4} \equiv (7^{2\text{^}3})^2 \equiv 12^2 \equiv 6 \pmod{23}$
  - $7^{2\text{^}5} \equiv (7^{2\text{^}4})^2 \equiv 6^2 \equiv 13 \pmod{23}$
  - $7^{2\text{^}6} \equiv (7^{2\text{^}5})^2 \equiv 13^2 \equiv 8 \pmod{23}$
  - $7^{2\text{^}7} \equiv (7^{2\text{^}6})^2 \equiv 8^2 \equiv 18 \pmod{23}$
  - $7^{2\text{^}8} \equiv (7^{2\text{^}7})^2 \equiv 18^2 \equiv 2 \pmod{23}$
  - $7^{2\text{^}9} \equiv (7^{2\text{^}8})^2 \equiv 2^2 \equiv 4 \pmod{23}$
- Use the last two parts to get 7^{1000} (mod 23)
  - $7^{1000} = 7^{2\text{^}9} * 7^{2\text{^}8} * 7^{2\text{^}7} * 7^{2\text{^}6} * 7^{2\text{^}5} * 7^{2\text{^}3}$

    $\equiv 4 * 2 * 18 * 8 * 13 * 12 \equiv 179712 \pmod{23} \equiv 13 \pmod{23}$

For which m is it the case that $(\forall a \in \mathbb{Z})[a^m \equiv a \pmod{m}]$?

Fermat's Little Theorem: If p is prime and a is an integer not divisible by p, then

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

Furthermore, for every integer a we have

$$a^p \equiv a \pmod{p}$$