Berkeley Math Circle
September 2022

Review of Modular Arithmetic

1. $12 \equiv 2 \pmod 5$

$12 \equiv 0 \pmod 6$

2. $-3 \equiv 2 \pmod 5$

$-3 \equiv 4 \pmod 7$

$89 \equiv 4 \pmod 5$

$-89 \equiv 1 \pmod 5$

3. $x - 3 \equiv 1 \pmod 5$ ➔ $x \equiv 4 \pmod 5$
4. $x + 2 \equiv 4 \pmod 5$ ➔ $x \equiv 2 \pmod 5$
5. $2x \equiv 3 \pmod 5$ ➔ $4x \equiv 6 \equiv 1 \pmod 5$
6. $2x \equiv 8 \pmod 5$ ➔ $x \equiv 4 \pmod 5$

   $3x \equiv 2 \pmod 5$ ➔ $2(3x) \equiv 6x \equiv \mathbf{x} \pmod 5$

   $2(2) \equiv \mathbf{4} \pmod 5$ So, $x \equiv 4 \pmod 5$
7. $2x \equiv 4 \pmod 5$ ➔ $x \equiv 2 \pmod 5$
8. $3x \equiv 3 \pmod 6$ ➔ x NOT $\equiv 1 \pmod 6$

   Check: $x = \mathbf{3}$ works since $9 \equiv 3 \pmod 6$

   but **3** NOT $\equiv 1 \pmod 6$

   However, $3x/3 = x \equiv 3/3 \equiv 1 \pmod{6/3} \equiv 1 \pmod 2$

   $\mathbf{3 \equiv 3 \pmod 6}$ $\mathbf{5 \times 3 = 15 \equiv 3 \pmod 6}$

   $\mathbf{7 \times 3 = 21 \equiv 3 \pmod 6}$

Solving Equations

1) $\mathbf{2x \equiv 1 \pmod 3}$

Since $(2, 3) = 1$, there is only one solution among 0, 1, 2 which is $x = 2$. And then any $\mathbf{x=2+(3k)}$, where k = integers, would satisfy this equation.

They are: $\{\ldots, -4, -1, 2, 5, 8, 11, \ldots\}$.

$2(2x) = 4x \equiv 2(1) \pmod 3$ ➔ $\mathbf{x \equiv 2 \pmod 3}$.

2) $\mathbf{8x \equiv 4 \pmod{12}}$

This implies $2x \equiv 1 \pmod 3$ since $(8, 12) = 4$ and the answers are:

$\{\ldots, -4, -1, 2, 5, 8, 11, \ldots\}$.

$2(2x) = 4x \equiv 2(1) \pmod 3 \equiv 2 \pmod 3$ ➔ $\mathbf{x \equiv 2 \pmod 3}$.

3) $\mathbf{6x \equiv 9 \pmod{15}}$

This implies $2x = 3 \pmod 5$ since $(6, 15) = 3$. Simple check to see that, among 0, 1, 2, 3, and 4, $x = 4$ works. So, $\mathbf{x = 4+5k}$ satisfy the equation. They are: $\{-6, -1, 4, 9, 14, \ldots\}$

$3(2x) = 6x \equiv 3(3) \pmod 5 \equiv 9 \pmod 5$ ➔ $\mathbf{x \equiv 4 \pmod 5}$.

4) $\mathbf{6x \equiv 2 \pmod 7}$

Since $(6, 7) = 1$, there is only one solution among 0, 1, 2, 3, 4, 5, and 6 which is $x = 5$. So, $\mathbf{x = 5+7k}$ satisfy the equation. They are: $\{.., -9, -2, 5, 12, 19, \ldots\}$

$6(6x) = 36x \equiv 6(2) \pmod 7 \equiv 12 \pmod 7$ ➔ $\mathbf{x \equiv 5 \pmod 7}$.

<u>Solving Equations</u>

5) $\mathbf{8x \equiv 2 \pmod{12}}$

This implies $\mathbf{4x \equiv 1 \pmod{6}}$. However, none of 0, 1, 2, 3, 4, 5 works. **No solution**.

6) $\mathbf{8x \equiv 5 \pmod{12}}$

None of 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 works.

No solution.

$ax \equiv c \pmod{m}$ has solution only if the GCD (a, m) is a factor of c.

7) $\mathbf{8x \equiv 4 \pmod{12}}$ ➔ $\mathbf{2x \equiv 1 \pmod{3}}$ $\quad \mathbf{x = 2+3k}$

$\mathbf{x = 5}$ $\qquad \mathbf{8(5) = 40 \equiv 4 \pmod{12}}$

$2(2x) = 4x \equiv 2(1) \pmod{3}$ ➔ $\mathbf{x \equiv 2 \pmod{3}}$.

DIVISIBILITY

x^2 from

Representation of whole numbers

123,456,789

9 = units digit

8 = tens digit

7 = hundreds digit

6 = thousands digit

5 = ten thousands digit

4 = hundred thousands digit

3 = millions digit

2 = ten millions digit

1 = hundred millions digit

123,456,789

9 = units digit	$= 1 = 10^0$
8 = tens digit	$= 10 = 10^1$
7 = hundreds digit	$= 100 = 10^2$
6 = thousands digit	$= 10^3$
5 = ten thousands digit	$= 10^4$
4 = hundred thousands digit	$= 10^5$
3 = millions digit	$= 10^6$
2 = ten millions digit	$= 10^7$
1 = hundred millions digit	$= 10^8$

123,456,789 =

$$\mathbf{1}\times10^8 + \mathbf{2}\times10^7 + \mathbf{3}\times10^6 + \mathbf{4}\times10^5 + \mathbf{5}\times10^4 + \mathbf{6}\times10^3 + \mathbf{7}\times10^2 + \mathbf{8}\times10^1 + \mathbf{9}\times10^0$$

Any number $\boldsymbol{m}$ can be represented by

$$\overline{\boldsymbol{a}_n \cdots \boldsymbol{a}_2 \boldsymbol{a}_1 \boldsymbol{a}_0}$$

or

$$\boldsymbol{m} = \boldsymbol{a}_n \times 10^n + \boldsymbol{a}_{n\text{-}1} \times 10^{n-1} + \ldots + \boldsymbol{a}_2 \times 10^2 + \boldsymbol{a}_1 \times 10^1 + \boldsymbol{a}_0 \times 1$$

So,

34067

$$= \overline{34067}$$

$$= \mathbf{3}\times10^4 + \mathbf{4}\times10^3 + \mathbf{0}\times10^2 + \mathbf{6}\times10^1 + 7\times1$$

Divisible by 2:

$$10^0 = 1 \equiv 1 \pmod{2}$$
$$10^k \equiv 0 \pmod{2} \quad k > 0$$

So, any number

$$\begin{aligned} \boldsymbol{m} &= \boldsymbol{a_n}\times 10^n + \boldsymbol{a_{n-1}}\times 10^{n-1} + \ldots + \boldsymbol{a_2}\times 10^2 + \boldsymbol{a_1}\times 10^1 + \boldsymbol{a_0}\times 1 \\ &\equiv \boldsymbol{a_n}\times 0 + \boldsymbol{a_{n-1}}\times 0 + \ldots + \boldsymbol{a_2}\times 0 + \boldsymbol{a_1}\times 0 + \boldsymbol{a_0}\times 1 \pmod{2} \\ &\equiv \boldsymbol{a_0} \pmod{2} \end{aligned}$$

Therefore, ***m*** is divisible by 2 if the units digit a_0 is ***even.***

<u>Divisible by 2:</u>

21345 is <u>not</u> divisible by 2 because 5 is not *even*.

23458 is divisible by 2 because 8 is *even*.

Divisible by 3:

$$10^k \equiv 1 \pmod 3 \quad k \geq 0$$

So, any number

$$\begin{aligned} \boldsymbol{m} &= \boldsymbol{a_n} \times 10^n + \boldsymbol{a_{n-1}} \times 10^{n-1} + \ldots + \boldsymbol{a_2} \times 10^2 + \boldsymbol{a_1} \times 10^1 + \boldsymbol{a_0} \times 1 \\ &\equiv \boldsymbol{a_n} \times 1 + \boldsymbol{a_{n-1}} \times 1 + \ldots + \boldsymbol{a_2} \times 1 + \boldsymbol{a_1} \times 1 + \boldsymbol{a_0} \times 1 \pmod 3 \\ &\equiv \boldsymbol{a_n} + \boldsymbol{a_{n-1}} + \ldots + \boldsymbol{a_2} + \boldsymbol{a_1} + \boldsymbol{a_0} \pmod 3 \end{aligned}$$

Therefore, ***m*** is divisible by 3 if the **sum** of all its digits is divisible by 3**.**

Divisible by 3:

21347 is not divisible by 3 because 2+1+3+4+7 = 17 is not divisible by 3.

22458 is divisible by 3 because 2+2+4+5+8 = 21 is divisible by 3.

Divisible by 4:

$$10^k \equiv 0 \pmod 4 \quad \text{if } k > 1$$

Any number

$$\begin{aligned} \boldsymbol{m} &= \boldsymbol{a_n}\times 10^n + \boldsymbol{a_{n-1}}\times 10^{n-1} + \ldots + \boldsymbol{a_2}\times 10^2 + \boldsymbol{a_1}\times 10^1 + \boldsymbol{a_0}\times 1 \\ &\equiv \boldsymbol{a_n}\times 0 + \boldsymbol{a_{n-1}}\times 0 + \ldots + \boldsymbol{a_2}\times 0 + \boldsymbol{a_1}\times 10 + \boldsymbol{a_0}\times 1 \pmod 4 \\ &\equiv \boldsymbol{a_1}\times 10 + \boldsymbol{a_0}\times 1 \pmod 4 \\ &\equiv \overline{\boldsymbol{a_1 a_0}} \pmod 4 \end{aligned}$$

Therefore, ***m*** is divisible by 4 if the number formed by the last two digits is divisible by 4.

Divisible by 4:

22458 is <u>not</u> divisible by 4 because 58 is <u>not</u> divisible by 4.

13524 is divisible by 4 because 24 is divisible by 4.

Divisible by 5:

$$10^0 \equiv 1 \pmod 5$$

$$10^k \equiv 0 \pmod 5 \quad \text{if } k > 0$$

Any number

$$\begin{aligned} \boldsymbol{m} &= \boldsymbol{a_n}\times 10^n + \boldsymbol{a_{n\text{-}1}}\times 10^{n\text{-}1} + \ldots + \boldsymbol{a_2}\times 10^2 + \boldsymbol{a_1}\times 10^1 + \boldsymbol{a_0}\times 1 \\ &\equiv \boldsymbol{a_n}\times 0 + \boldsymbol{a_{n\text{-}1}}\times 0 + \ldots + \boldsymbol{a_2}\times 0 + \boldsymbol{a_1}\times 0 + \boldsymbol{a_0}\times 1 \pmod 5 \\ &\equiv \boldsymbol{a_0} \pmod 5 \end{aligned}$$

Therefore, ***m*** is divisible by 5 if the last digit is either 0 or 5.

<u>**Divisible by 5:**</u>

22458 is <u>not</u> divisible by 5 because 8 is <u>not</u> 0 or 5.

13520 and 13525 are both divisible by 5 because their last digit is 0 or 5.

Divisible by 6:

A number that is divisible by 6 must be divisible by both 2 and 3. So, this number must be:

1. Even number, and
2. The sum of all its digits is divisible by 3.

Divisible by 6:

21453 is not divisible by 6 because the last digit 3 is odd (although 2+1+4+5+3 = 15 is divisible by 3).

13520 is not divisible by 6 because 1+3+5+2+0 = 11 is not divisible by 3.

13524 is divisible by 6 because the last digit is even and 1+3+5+2+4 = 15 is divisible by 3.

Divisible by 8:

$$10^k \equiv 0 \pmod{8} \quad \text{if } k > 2$$

Any number

$$\begin{aligned} \boldsymbol{m} &= \boldsymbol{a_n}\times 10^n + \boldsymbol{a_{n-1}}\times 10^{n-1} + \ldots + \boldsymbol{a_2}\times 10^2 + \boldsymbol{a_1}\times 10^1 + \boldsymbol{a_0}\times 1 \\ &\equiv \boldsymbol{a_n}\times 0 + \boldsymbol{a_{n-1}}\times 0 + \ldots + \boldsymbol{a_3}\times 0 + \boldsymbol{a_2}\times 100 + \boldsymbol{a_1}\times 10 + \boldsymbol{a_0}\times 1 \pmod{8} \\ &\equiv \boldsymbol{a_2}\times 100 + \boldsymbol{a_1}\times 10 + \boldsymbol{a_0}\times 1 \pmod{8} \\ &\equiv \overline{\boldsymbol{a_2 a_1 a_0}} \pmod{8} \end{aligned}$$

Therefore, ***m*** is divisible by 8 if the number formed by the last three digits is divisible by 8.

Divisible by 8:

13022458 is not divisible by 8 because 458 is not divisible by 8.

13022456 is divisible by 8 because 456 is divisible by 8.

Divisible by 9:

$$10^k \equiv 1 \pmod 9 \quad k \geq 0$$

So, any number

$$\begin{aligned} \boldsymbol{m} &= \boldsymbol{a_n} \times 10^n + \boldsymbol{a_{n-1}} \times 10^{n-1} + \ldots + \boldsymbol{a_2} \times 10^2 + \boldsymbol{a_1} \times 10^1 + \boldsymbol{a_0} \times 1 \\ &\equiv \boldsymbol{a_n} \times 1 + \boldsymbol{a_{n-1}} \times 1 + \ldots + \boldsymbol{a_2} \times 1 + \boldsymbol{a_1} \times 1 + \boldsymbol{a_0} \times 1 \pmod 9 \\ &\equiv \boldsymbol{a_n} + \boldsymbol{a_{n-1}} + \ldots + \boldsymbol{a_2} + \boldsymbol{a_1} + \boldsymbol{a_0} \pmod 9 \end{aligned}$$

Therefore, ***m*** is divisible by 9 if the **sum** of all its digits is divisible by 9.

Divisible by 10:

$$10^{0} \equiv 1 \pmod{10}$$
$$10^{k} \equiv 0 \pmod{10} \quad k \geq 1$$

So, any number

$$\begin{aligned} \boldsymbol{m} &= \boldsymbol{a_n}\times 10^{n} + \boldsymbol{a_{n-1}}\times 10^{n-1} + \ldots + \boldsymbol{a_2}\times 10^{2} + \boldsymbol{a_1}\times 10^{1} + \boldsymbol{a_0}\times 1 \\ &\equiv \boldsymbol{a_n}\times 0 + \boldsymbol{a_{n-1}}\times 0 + \ldots + \boldsymbol{a_2}\times 0 + \boldsymbol{a_1}\times 0 + \boldsymbol{a_0}\times 1 \pmod{10} \\ &\equiv \boldsymbol{a_0} \pmod{10} \end{aligned}$$

Therefore, ***m*** is divisible by 10 if the last digit is divisible by 10 which means the last digit ends in 0.

Divisible by 10:

21345 is not divisible by 10 because the last digit (5) is not 0.

21340 is divisible by 10 because the last digit is 0.

Divisible by 11:

$10^k \equiv 1 \pmod{11}$ if k is even

$10^k \equiv 10 \pmod{11} \equiv -1 \pmod{11}$ if k is odd

So, any number

$$\boldsymbol{m} = \boldsymbol{a_n}\times 10^n + \boldsymbol{a_{n-1}}\times 10^{n-1} + \ldots + \boldsymbol{a_2}\times 10^2 + \boldsymbol{a_1}\times 10^1 + \boldsymbol{a_0}\times 1$$

$$\equiv \boldsymbol{a_n}\times(\pm 1) + \boldsymbol{a_{n-1}}\times(\pm 1) + \ldots + \boldsymbol{a_2}\times 1 + \boldsymbol{a_1}\times(-1) + \boldsymbol{a_0}\times 1 \pmod{11}$$

$$\equiv \pm\, \boldsymbol{a_n} \pm \boldsymbol{a_{n-1}} + \ldots + \boldsymbol{a_2} - \boldsymbol{a_1} + \boldsymbol{a_0} \pmod{11}$$

$$\equiv \boldsymbol{a_n} - \boldsymbol{a_{n-1}} + \ldots + \boldsymbol{a_2} - \boldsymbol{a_1} + \boldsymbol{a_0} \pmod{11} \quad \text{or}$$

$$\equiv -\boldsymbol{a_n} + \boldsymbol{a_{n-1}} - \ldots + \boldsymbol{a_2} - \boldsymbol{a_1} + \boldsymbol{a_0} \pmod{11}$$

Therefore, ***m*** is divisible by 11 if the difference of the sum of alternative digits is divisible by 11.

Divisible by 11:

21317 is <u>not</u> divisible by 11 because (2+3+7) – (1+1) = 10 is <u>not</u> divisible by 11.

21307 is divisible by 11 because (2+3+7) – (1+0) = 11 is divisible by 11.

Divisible by 12:

A number that is divisible by 12 must be divisible by both 4 and 3. So, this number must be:

1. Last 2 digits divisible by 4, and
2. The sum of all its digits is divisible by 3.

<u>Divisible by 12:</u>

21453 is <u>not</u> divisible by 12 because the last digit 3 is odd (although 2+1+4+5+3 = 15 is divisible by 3).

13520 is <u>not</u> divisible by 12 because 1+3+5+2+0 = 11 is not divisible by 3 (although 20 is divisible by 4).

13524 is divisible by 12 because the last digit is even and 1+3+5+2+4 = 15 is divisible by 3 and 24 is divisible by 4.

Divisible by 7:

$5 \times 10 \equiv 1 \pmod 7$

$5 \equiv -2 \pmod 7$

So, any number

$$\boldsymbol{m} = \overline{\boldsymbol{a_n \ldots a_2 a_1 a_0}}$$

$$5 \times m = 5 \times (\overline{\boldsymbol{a_n \ldots a_2 a_1 a_0}})$$

$$= 50 \times (\overline{\boldsymbol{a_n \ldots a_2 a_1}}) + 5 \times \boldsymbol{a_0}$$

$$\equiv (\overline{\boldsymbol{a_n \ldots a_2 a_1}}) + 5 \times \boldsymbol{a_0} \pmod 7$$

$$\equiv (\overline{\boldsymbol{a_n \ldots a_2 a_1}}) - 2 \times \boldsymbol{a_0} \pmod 7$$

Divisible by 7:

If the result of multiplying the last digit by 2 and the product is subtracted from the rest of the number is either 0 or divisible by 7, then this number is divisible by 7.

Examples:

(1) **861**. 86 – 2×1 = 84 is divisible by 7 so 861 is divisible by 7.

(2) **8638**. 863 – 2×8 = 847. Is 847 divisible by 7?
84 – 2×7 = 70 is divisible by 7 so the original number 8638 is divisible by 7.

Divisible by 13:

$40 \equiv 1 \pmod{13}$

So, any number

$\boldsymbol{m} = \overline{\boldsymbol{a_n \ldots a_2 a_1 a_0}}$. Let $\boldsymbol{k} = \overline{\boldsymbol{a_n \ldots a_2 a_1}}$.

Then, $\boldsymbol{m} = 10\boldsymbol{k} + \boldsymbol{a_0}$.

$$\begin{aligned} 4\times\boldsymbol{m} &= 40\times\boldsymbol{k} + 4\times\boldsymbol{a_0} \\ &\equiv \boldsymbol{k} + 4\times\boldsymbol{a_0} \pmod{13} \\ &\equiv \boldsymbol{k} - 9\times\boldsymbol{a_0} \pmod{13} \end{aligned}$$

$\boldsymbol{m}$ is divisible by 13 if $4\boldsymbol{m}$ is divisible by 13.

Divisible by 13:

If the result of multiplying the last digit by 9 and the product is subtracted from the rest of the number is divisible by 13, then this number is divisible by 13.

Examples:

(1) **13261**. $1326 - 9\times1 = 1317$ and $131 - 9\times7 = 68$ is not divisible by 13 so 13261 is not divisible by 13.

(2) **13260**. $1326 - 9\times0 = 1326$ and $132 - 9\times6 = 78$ is divisible by 13 so 13260 is divisible by 13.

LINEAR DIOPHANTINE EQUATIONS

Solve $17x + 11y = 73$. If x and y could be any numbers, there are infinite number of solutions.

For example: When $\boldsymbol{x=0}$, $11y=73$ or $\boldsymbol{y=73/11}$. When $\boldsymbol{x=3}$, $11y=22$ or $\boldsymbol{y=2}$. However, Diophantine Equations require x and y to be integers.

This equation is equivalent to the problem that asks Mr. Brown bought some apples at 17¢ each and some oranges at 11¢ each. He spent 73¢. How many of each kind did he buy?

LINEAR DIOPHANTINE EQUATIONS

Solve $17x + 11y = 73$.

By chance, we found $(x, y) = (3, 2), (14, -15), (-8, 19)$. There are many others. Can you see a pattern?

LINEAR DIOPHANTINE EQUATIONS

Solve $17x + 11y = 73$.

By chance, we found $(x, y) = (3, 2), (14, -15), (-8, 19)$. There are many others. Can you see a pattern?

$17x = 73 - 11y$ $\quad 17x \equiv \mathbf{6x} \pmod{11}$ and $73 \equiv \mathbf{7} \pmod{11}$

$\mathbf{6x} \equiv \mathbf{7} \pmod{11} \equiv 18 \pmod{11}$ $\quad$ or $\quad x \equiv 3 \pmod{11}$

So, $\boldsymbol{x = 3+11k}$ $\quad$ $\boldsymbol{k}$ **= integers**

$11y = 73 - 17x$ $\quad 11y \equiv \mathbf{11y} \pmod{17}$ and $73 \equiv \mathbf{5} \pmod{17}$

$\mathbf{11y} = 73 - 17x = 73 - 17(\mathbf{3+11k}) = 73 - 51 - 187\boldsymbol{k} \mathbf{=} 22 - 187\boldsymbol{k}$

or $\boldsymbol{y = 2 - 17k}$ $\quad$ $\boldsymbol{k}$ **= integers**

LINEAR DIOPHANTINE EQUATIONS

Solve $3x + 5y = 28$.

$3x = 28 - 5y$ $3x \equiv \mathbf{3x} \pmod 5$ and $28 \equiv \mathbf{3} \pmod 5$

$\mathbf{3x} \equiv \mathbf{3} \pmod 5$ or $x \equiv 1 \pmod 5$ or $\boldsymbol{x = 1+5k}$

$5y = 28 - 3(1+5k)$ $5y = 25 - 15k$

$y = 5 - 3k$ or $\boldsymbol{y \equiv 5-3k}$ k = integers.

Not all equations $ax + by = c$ have integer solutions.
It has integer solutions only if GCD(a, b) is a factor of c.

1. $13x + 11y = 17$
2. $91x - 26y = 3$
3. $73x - 17y = 62$
4. $x^2 - y^2 = 2002$
5. $x^4 - 4y = 3$
6. $a^{154} - 1$ is divisible by 23 $\text{GCD}(a, 23) = 1$
7. $a^{80} - 1$ is divisible by 17 $\text{GCD}(a, 17) = 1$
8. Remainder when 3^{50} is divided by 7
9. Remainder when 221^{2012} is divided by 9

1. $\mathbf{13x + 11y = 17}$ **GCD(13, 11) = 1**

$13x = 17 - 11y \quad 2x \equiv 6 \pmod{11} \quad x \equiv 3 \pmod{11}$

$\mathbf{x = 3 + 11k}$

$11y = 17 - 13x = 17 - 13(\mathbf{3 + 11k}) = 17 - 39 - 143k = -22 - 13k$

$\mathbf{y = -2 - 13k}$

2. $\mathbf{91x - 26y = 3}$

GCD(91, 26) = 13 but 13 is not a factor of 3.

No solution in integers.

3. $\mathbf{73x - 17y = 62}$ **GCD(73, 17) = 1**

$73x = 62 + 17y \quad 5x \equiv 11 \pmod{17} \quad 5x \equiv 45 \pmod{17}$

(or $7(5x) \equiv 7(11) \pmod{17} \quad 35x \equiv 77 \pmod{17}$) $\quad x \equiv 9 \pmod{17}$

$\mathbf{x = 9 + 17k}$

$17y = -62 + 73x = -62 + 73(\mathbf{9 + 17k}) = 595 + 1241k$

$y \equiv 35 \pmod{73}$

$\mathbf{y = 35 + 73k}$

4. $\boldsymbol{x^2 - y^2 = 2002}$

$x^2 \equiv 0$ or $1 \pmod 4$ $y^2 \equiv 0$ or $1 \pmod 4$

So $x^2 - y^2 \equiv 0, 1, -1 \pmod 4$.

But $2002 \equiv 2 \pmod 4$ **No integer solution**.

$(x-y)(x+y) = 2002 = 2\times7\times11\times13$

Lots possibilities: $x-y=1/x+y=2002$ or $x-y=2/x+y=1001$

or …

5. $\boldsymbol{x^4 - 4y = 3}$

No integer solution. $x^4 \equiv 3 \pmod 4$. But

$x^4 \equiv 0$ or $1 \pmod 4$

FERMAT's LITTLE THEOREM (p = prime number)

a is an integer ≥ 1. Then $a^p \equiv a \pmod{p}$

a is an integer ≥ 1 and $(a, p)=1$. Then $a^{p-1} \equiv 1 \pmod{p}$.

$2^{5-1} = 2^4 \equiv 1 \pmod{5}$

$2^7 \equiv 2 \pmod{7}$

$2^{29} \equiv 2 \pmod{29}$

$10^{10} \equiv 1 \pmod{11}$

$10^5 \equiv 10 \pmod{5}$ but 10^4 **NOT** $\equiv 1 \pmod{5}$

2^4 **NOT** $\equiv 2 \pmod{4}$ $4 \neq$ prime

6^{3-2} **NOT** $\equiv 1 \pmod{3}$ $(6, 3) \neq 1$

FERMAT's LITTLE THEOREM

(p = prime number and a = integer between 1 and p)

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

Proof (Use Modular Arithmetic):

Fact: $\{a, 2a, 3a, \ldots, (p-1)a\}$ is a re–arrangement of $\{1, 2, 3, \ldots, (p-1)\}$

$\{4, 2(4), 3(4), 4(4)\} = \{4, 8, 12, 16\} \equiv \{4, 3, 2, 1\}$ $\quad p = 5, a = 4$

$$a \times 2a \times 3a \times \ldots \times (p-1)a = a^{p-1}(p-1)!$$

$$1 \times 2 \times 3 \times \ldots \times (p-1) = (p-1)!$$

So $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$ and $a^{p-1} \equiv 1 \pmod{p}$

FERMAT's LITTLE THEOREM

(p = prime number and a = integer between 1 and p)

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

Proof (Use Induction):

Fact: $(x + y)^p \equiv x^p + y^p \pmod p$

Use Induction: Want to prove $a^p \equiv a \pmod p$.

a=1 is obviously true.

Assume $a^p \equiv a \pmod p$.

$(a+1)^p \equiv a^p + 1^p \pmod p \equiv a+1 \pmod p$.

6. **a^{154} –1 is divisible by 23   GCD(a, 23) = 1**

$a^{22} \equiv 1 \pmod{23}$ $a^{154} = (a^{22})^7 \equiv 1^7 \equiv 1 \pmod{23}$

7. **a^{80} –1 is divisible by 17   GCD(a, 17) = 1**

$a^{16} \equiv 1 \pmod{17}$ $a^{80} = (a^{16})^5 \equiv 1^5 \equiv 1 \pmod{17}$

8. **Remainder when 3^{50} is divided by 7**

$3^6 \equiv 1 \pmod 7$ $(3^6)^8 \equiv 1 \pmod 7$

$3^{50} = (3^{48})(3^2) \equiv (1)(9) \pmod 7 \equiv 2 \pmod 7$

9. **Remainder when 221^{2012} is divided by 9**

$221^1 \equiv 5 \pmod 9$

$221^2 \equiv 7 \pmod 9$

$221^3 \equiv 8 \pmod 9$

$221^4 \equiv 4 \pmod 9$

$221^5 \equiv 2 \pmod 9$

$221^6 \equiv 1 \pmod 9$

$221^7 \equiv 5 \pmod 9$ Every 6 repeats

$2012 \equiv 2 \pmod 6$. So, remainder should be 7.

Applications

Joanne was expecting six guests and wanted to give them each a bag of candies. Wanting to be fair to all, she divided the candies into 6 equal piles and found that they came out even. Just before the party was to begin a guest called to ask if he might bring a friend. Hence Joanne had to divide the candies into 7 piles; here she found she had two left over. What is the least number of candies she could have had?

$6n \equiv 2 \pmod{7}$. Upon checking, among the numbers 0, 1, 2, 3, 4, 5, 6, only 5 works. So, the answers are: $\{5, 12, 19, 26, \ldots\}$. So the least number is $6n = 6\times5 = 30$ pieces of candies.

Applications Cryptography I

Caesar Cipher Shifting the alphabet forward 3 places.

a–>d, b–>e, c–>f, d–>g, … , w–>z, x–>a, y–>b, z–>c.

How to send out this message?
attack.

Applications

Cryptography I

Caesar Cipher Shifting the alphabet forward 3 places.

a–>d, b–>e, c–>f, … , w–>z, x–>a, y–>b, z–>c.

What is **wklvphvvdjhlvwrsvhfuhw**?

Applications
Cryptography I

Caesar Cipher Shifting the alphabet forward 3 places.
a–>d, b–>e, c–>f, … , w–>z, x–>a, y–>b, z–>c.

To decipher, shift the alphabets backward 3 places.

Replace letters with numbers: a=0, b=1, c=2, … , w=22, x=23, y=24, z=25

Examples:
To send a secret message: D ≡ (E+3) (mod 26)
x=23 (E number), so the corresponding E number is D=(23+3)= 26≡ 0 (mod 26) 0=a.
k=10 (E number), so the corresponding E number is D=(10+3)≡13 (mod 26) 13= n

To decipher a secret message: E ≡ (D–3) (mod 26)
w=22 (D number), so the corresponding E number is E=(22–3) ≡ 19 (mod 26) 19=t.
k=10 (D number), so the corresponding E number is E=(10–3)≡7 (mod 26) 7= h
b=1 (D number), so the corresponding E number is E=(1–3)=–2≡24(mod 26) 24=y.

3 = Key $K_E = 3$ $K_D = -3$

Applications
Cryptography II

Improved Caesar Cipher Multiply 5 times.

Replace letter s with numbers: a=0, b=1, c=2, … , w=22, x=23, y=24, z=25

5a = 0 –>a, 5b=5–>f, 5c=10–>k, … , 5w=110≡6–>g, 5x=115≡11–>l, 5y=120≡16–>q, 5z=125–>v.

How to send out the message **attack** ?

Applications
Cryptography II

Improved Caesar Cipher Multiply 5 times.
Replace letter s with numbers: a=0, b=1, c=2, … , w=22, x=23, y=24, z=25

5a = 0 –>a, 5b=5–>f, 5c=10–>k, … , 5w=110≡6–>g, 5x=115≡11–>l, 5y=120≡16–>q, 5z=125–>v.

What is **euriuaioddosngsnm?**

To decipher, divide by 5.

Examples:
To send a secret message: D ≡ 5E (mod 26)
x=23 (E number), so the corresponding E number is
D=5×23= 115≡ 11 (mod 26) 11=l.
k=10 (E number), so the corresponding E number is
D=5×10≡50≡24 (mod 26) 24= q

Applications
Cryptography II

Improved Caesar Cipher Multiply 5 times.

Replace letter s with numbers: a=0, b=1, c=2, … , w=22, x=23, y=24, z=25 **eursuaioddosngsnm**

To decipher a secret message: Must find the multiplicative inverse of 5 so that $E \equiv 1/5D \pmod{26} \equiv 21D \pmod{26}$

e=4 (D number), so the corresponding E number is $E=21\times4=84\equiv6 \pmod{26}$ 6=g.

u=20 (D number), so the corresponding E number is $E=21\times20=420\equiv4 \pmod{26}$ 4= e

5 = key $K_E = 5$ $K_D = 21$

Applications

Cryptography III

Can we use $K_E = 4$?

Applications

Cryptography III

Can we use $K_E = 4$?

$4 \times 3 = 12$ d -> m

$4 \times 16 = 64 \equiv 12 \pmod{26}$ q -> m

Applications

Cryptography IV

General encipherment rule:

$D \equiv (mE+s) \pmod{26}$

m=5, s=18 $D \equiv (5E+18) \pmod{26}$

{0, 1, 2, 13, 25} –> {18, 23, 2, 5, 13}

{a, b, c, n, z} –> {s, x, c, f, n}

Applications
Cryptography V

Bigger is Better

Divide into groups of 2:

I want a million dollars –>

iw an ta mi ll io nd ol la rs

$D \equiv (mE+s) \pmod{26\times 26=676}$

aa=0, ab=1, ac=2, …, zy=674, zz=675

Applications

Cryptography V

I want your dollar –>

iw an ty ou rd ol la r

Applications

Cryptography V

I want your dollar –>

iw an ty ou rd ol la r!

$D \equiv (mE+s) \pmod{26\times27=702}$

aa=0, ab=1, ac=2, …az=25, a!=26, ba=27, zy=699, zz=700, z!=701