# Puzzles, Surprises, IMO, and Number Theory

Dr. Koopa Koo

Hong Kong International Mathematical Olympiad Committee
email: dr.koopakoo@gmail.com

April 22, 2010

The International Mathematical Olympiad (IMO) is for pre-university students and is the oldest of the International Science Olympiads. The first IMO was held in Romania in 1959. It has since been held annually, except in 1980. About 100 countries send teams of up to six students.

1. IMO is considered to be the most important and influential mathematical competition at the secondary level.
2. It is a two-day contest, 4.5 hours per day.
3. The paper consists of 6 problems, 3 per day.
4. Each problem worth 7 points, thus the full score is 42 points.

The International Mathematical Olympiad (IMO) is for pre-university students and is the oldest of the International Science Olympiads. The first IMO was held in Romania in 1959. It has since been held annually, except in 1980. About 100 countries send teams of up to six students.

1. IMO is considered to be the most important and influential mathematical competition at the secondary level.
2. It is a two-day contest, 4.5 hours per day.
3. The paper consists of 6 problems, 3 per day.
4. Each problem worth 7 points, thus the full score is 42 points.

The International Mathematical Olympiad (IMO) is for pre-university students and is the oldest of the International Science Olympiads. The first IMO was held in Romania in 1959. It has since been held annually, except in 1980. About 100 countries send teams of up to six students.

1. IMO is considered to be the most important and influential mathematical competition at the secondary level.
2. It is a two-day contest, 4.5 hours per day.
3. The paper consists of 6 problems, 3 per day.
4. Each problem worth 7 points, thus the full score is 42 points.

The International Mathematical Olympiad (IMO) is for pre-university students and is the oldest of the International Science Olympiads. The first IMO was held in Romania in 1959. It has since been held annually, except in 1980. About 100 countries send teams of up to six students.

1. IMO is considered to be the most important and influential mathematical competition at the secondary level.
2. It is a two-day contest, 4.5 hours per day.
3. The paper consists of 6 problems, 3 per day.
4. Each problem worth 7 points, thus the full score is 42 points.

**The four basic areas.**

1. Algebra
2. Combinatorics
3. Geometry
4. Number Theory

□

**The four basic areas.**

1. Algebra
2. Combinatorics
3. Geometry
4. Number Theory

□

## Problems in the IMO

**The four basic areas.**

1. Algebra
2. Combinatorics
3. Geometry
4. Number Theory

□

**The four basic areas.**

1. Algebra
2. Combinatorics
3. Geometry
4. Number Theory

□

1. HKIMO Prelim (Coming up on 29th May) (Weight $= 1$)
2. Qualified students are invited to the IMO Training
3. Selection Test 1 (August) (Weight $= 2$)
4. Selection Test 2 (October) (Weight $= 3$)
5. CHKMO (December) (Weight $= 3$)
6. APMO (March) (Weight $= 4$)

1. HKIMO Prelim (Coming up on 29th May) (Weight $= 1$)
2. Qualified students are invited to the IMO Training
3. Selection Test 1 (August) (Weight $= 2$)
4. Selection Test 2 (October) (Weight $= 3$)
5. CHKMO (December) (Weight $= 3$)
6. APMO (March) (Weight $= 4$)

1. HKIMO Prelim (Coming up on 29th May) (Weight = 1)
2. Qualified students are invited to the IMO Training
3. Selection Test 1 (August) (Weight = 2)
4. Selection Test 2 (October) (Weight = 3)
5. CHKMO (December) (Weight = 3)
6. APMO (March) (Weight = 4)

1. HKIMO Prelim (Coming up on 29th May) (Weight $= 1$)
2. Qualified students are invited to the IMO Training
3. Selection Test 1 (August) (Weight $= 2$)
4. Selection Test 2 (October) (Weight $= 3$)
5. CHKMO (December) (Weight $= 3$)
6. APMO (March) (Weight $= 4$)

1. HKIMO Prelim (Coming up on 29th May) (Weight $= 1$)
2. Qualified students are invited to the IMO Training
3. Selection Test 1 (August) (Weight $= 2$)
4. Selection Test 2 (October) (Weight $= 3$)
5. CHKMO (December) (Weight $= 3$)
6. APMO (March) (Weight $= 4$)

1. HKIMO Prelim (Coming up on 29th May) (Weight $= 1$)
2. Qualified students are invited to the IMO Training
3. Selection Test 1 (August) (Weight $= 2$)
4. Selection Test 2 (October) (Weight $= 3$)
5. CHKMO (December) (Weight $= 3$)
6. APMO (March) (Weight $= 4$)

2010 Team Members

| | |
|---|---|
| Ching Tak Wing | Queen's College |
| Hung Ka Kin | Diocesan Boys' School (Caltech '14) |
| Chung Ping Ngai | LaSalle College (MIT '14) |
| Tam Ka Yu | Queen's College |
| Yu Tak Hei | LaSalle College |
| Yip Hok Pan | Ying Wa College |

2010 Reserved Team Members

| | |
|---|---|
| Lo Jing Hoi | LaSalle College |
| Kwok Hoi Kit | LaSalle College |
| Li Yau Wing | Ying Wa College |
| Wong Ching (F) | PLK Centenary Li Shiu Chung Mem College |
| Chan Kwun Tat | SKH Lam Woo Mem Sec School |
| Wo Bar Wai Barry | LaSalle College |

# What's Next

1. Primes
2. Euclidean Algorithm
3. Modular Arithmetic
4. Fermat's Little Theorem and the Cubing Lemma
5. Dirichlet's Theorem and the Chebotarev Density Theorem
6. Fermat's Last Theorem

# What's Next

1. Primes
2. Euclidean Algorithm
3. Modular Arithmetic
4. Fermat's Little Theorem and the Cubing Lemma
5. Dirichlet's Theorem and the Chebotarev Density Theorem
6. Fermat's Last Theorem

# What's Next

1. Primes
2. Euclidean Algorithm
3. Modular Arithmetic
4. Fermat's Little Theorem and the Cubing Lemma
5. Dirichlet's Theorem and the Chebotarev Density Theorem
6. Fermat's Last Theorem

1. Primes
2. Euclidean Algorithm
3. Modular Arithmetic
4. Fermat's Little Theorem and the Cubing Lemma
5. Dirichlet's Theorem and the Chebotarev Density Theorem
6. Fermat's Last Theorem

# What's Next

1. Primes
2. Euclidean Algorithm
3. Modular Arithmetic
4. Fermat's Little Theorem and the Cubing Lemma
5. Dirichlet's Theorem and the Chebotarev Density Theorem
6. Fermat's Last Theorem

# What's Next

1. Primes
2. Euclidean Algorithm
3. Modular Arithmetic
4. Fermat's Little Theorem and the Cubing Lemma
5. Dirichlet's Theorem and the Chebotarev Density Theorem
6. Fermat's Last Theorem

**Definition**

A positive integer is a *prime* number if it is only divisible by itself and 1. (Note 1 is NOT a prime number.)

**Theorem**

*There is no largest prime number, that is, there are infinitely many primes.*

**Proof.**

1. Suppose $p$ were the largest prime number.
2. Let $q$ be the product of the first $p$ numbers.
3. Then $q+1$ is not divisible by any of them.
4. Thus $q+1$ is also prime and greater than $p$. □

**Definition**

A positive integer is a *prime* number if it is only divisible by itself and 1. (Note 1 is NOT a prime number.)

**Theorem**

*There is no largest prime number, that is, there are infinitely many primes.*

**Proof.**

1. Suppose $p$ were the largest prime number.
2. Let $q$ be the product of the first $p$ numbers.
3. Then $q + 1$ is not divisible by any of them.
4. Thus $q + 1$ is also prime and greater than $p$.

□

**Definition**

A positive integer is a *prime* number if it is only divisible by itself and 1. (Note 1 is NOT a prime number.)

**Theorem**

*There is no largest prime number, that is, there are infinitely many primes.*

**Proof.**

1. Suppose $p$ were the largest prime number.
2. Let $q$ be the product of the first $p$ numbers.
3. Then $q + 1$ is not divisible by any of them.
4. Thus $q + 1$ is also prime and greater than $p$.

**Definition**

A positive integer is a *prime* number if it is only divisible by itself and 1. (Note 1 is NOT a prime number.)

**Theorem**

*There is no largest prime number, that is, there are infinitely many primes.*

**Proof.**

1. Suppose $p$ were the largest prime number.
2. Let $q$ be the product of the first $p$ numbers.
3. Then $q + 1$ is not divisible by any of them.
4. Thus $q + 1$ is also prime and greater than $p$. □

### A Natural Question

*Can we do better?*

The question is answered by the Prime Number Theorem.

### Definition

Let $\pi(x)$ denote the number of primes less than $x$. For example, $\pi(10) = 4$ since there are four primes, viz. $2, 3, 5, 7$ less than 10. Also, $\pi(100) = 25$.

### Theorem (Prime Number Theorem)

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

*In other words, when $x$ is big,*

$$\pi(x) \sim \frac{x}{\ln x}.$$

Euclidean Algorithm is basically repeated use of division algorithm and it is very handy in finding the gcd of two integers $a$ and $b$, denoted by $\gcd(a, b)$.

**Example**

*Find* $\gcd(121, 7)$.

**Solution.**

Write $121 = 7 \times 17 + 2$, then we have:

$$\begin{aligned} 121 &= 17 \times 7 + 2 \\ 7 &= 3 \times 2 + \boxed{1} \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

$(121, 7)$ is the least non-zero remainder, which is 1, thus $(121, 7) = 1$. □

**Theorem**

*For $a, b \in \mathbb{Z}$, with $\gcd(a, b) = 1$ then there exists $x, y \in \mathbb{Z}$ such that*

$$ax + by = 1.$$

For the previous example, in order to find the $x, y$ in the theorem. We run the algorithm backwards

**Solution.**

$$\begin{aligned} 1 &= 7 - 3 \times 2 \\ &= 7 - 3 \times (121 - 7 \times 17) \\ &= 7 - 3 \times 121 + 51 \times 7 \\ &= 52 \times 7 - 3 \times 121. \end{aligned}$$

Note that we replace 2 by $121 - 7 \times 17$ in the second line. Hence $x, y$ are $-3, 52$ respectively. □

**Example (IMO 1959 Q1)**

*Prove that* $\frac{21n+4}{14n+3}$ *is irreducible for every natural number* $n$.

**Proof.**

It suffices to prove that $\gcd(21n+4, 14n+3) = 1$ for all $n$.
Applying the Euclidean algorithm, we have:

$$\begin{aligned} 21n+4 &= 1 \times (14n+3) + (7n+1) \\ 14n+3 &= 2 \times (7n+1) + \boxed{1} \\ 7n+1 &= (7n+1) \times 1 + 0 \end{aligned}$$

Thus $\gcd(21n+4, 14n+3) = 1$ for all $n$. □

**Definition**

$a \equiv b \pmod{m}$ iff $m \mid a - b$, in which we say that $a$ is congruent to $b$ modulo $m$.

**Example**

*In congruence notation, we have*

1. $3 \equiv 1 \pmod{2}$,
2. $7 \equiv 4 \equiv 1 \equiv -2 \equiv 10 \pmod{3}$.

*Notice that $n$ is even iff $n \equiv 0 \pmod{2}$.*

**Definition**

$a \equiv b \pmod{m}$ iff $m \mid a - b$, in which we say that $a$ is congruent to $b$ modulo $m$.

**Example**

*In congruence notation, we have*

1. $3 \equiv 1 \pmod{2}$,
2. $7 \equiv 4 \equiv 1 \equiv -2 \equiv 10 \pmod{3}$.

*Notice that $n$ is even iff* $n \equiv 0 \pmod{2}$.

**Definition**

$a \equiv b \pmod{m}$ iff $m \mid a - b$, in which we say that $a$ is congruent to $b$ modulo $m$.

**Example**

*In congruence notation, we have*

1. $3 \equiv 1 \pmod{2}$,
2. $7 \equiv 4 \equiv 1 \equiv -2 \equiv 10 \pmod{3}$.

*Notice that $n$ is even iff $n \equiv 0 \pmod{2}$.*

### Theorem (Basic Properties of Congruence)

*Suppose* $a, b, c, d, m \in \mathbb{Z}$, *we have:*

1. $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$
2. $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow a \pm c \equiv b \pm d \pmod{m}$.
3. $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.
4. $ab \equiv ac \pmod{m}, \gcd(a, m) = 1 \Rightarrow b \equiv c \pmod{m}$.

**Theorem (Basic Properties of Congruence)**

*Suppose* $a, b, c, d, m \in \mathbb{Z}$*, we have:*

1. $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$
2. $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow a \pm c \equiv b \pm d \pmod{m}$.
3. $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.
4. $ab \equiv ac \pmod{m}, \gcd(a, m) = 1 \Rightarrow b \equiv c \pmod{m}$.

**Theorem (Basic Properties of Congruence)**

*Suppose* $a, b, c, d, m \in \mathbb{Z}$*, we have:*

1. $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$
2. $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow a \pm c \equiv b \pm d \pmod{m}$.
3. $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.
4. $ab \equiv ac \pmod{m}, \gcd(a, m) = 1 \Rightarrow b \equiv c \pmod{m}$.

**Theorem (Basic Properties of Congruence)**

*Suppose* $a, b, c, d, m \in \mathbb{Z}$*, we have:*

1. $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$
2. $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow a \pm c \equiv b \pm d \pmod{m}$.
3. $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.
4. $ab \equiv ac \pmod{m}, \gcd(a, m) = 1 \Rightarrow b \equiv c \pmod{m}$.

**Theorem (Basic Properties of Congruence)**

*Suppose* $a, b, c, d, m \in \mathbb{Z}$, *we have:*

1. $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$
2. $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow a \pm c \equiv b \pm d \pmod{m}$.
3. $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.
4. $ab \equiv ac \pmod{m}, \gcd(a, m) = 1 \Rightarrow b \equiv c \pmod{m}$.

## Example (IMO 1964 Q1)

*(a) Find all natural numbers $n$ for which 7 divides $2^n - 1$.*
*(b) Prove that there is no natural number $n$ for which 7 divides $2^n + 1$.*

## Proof.

(a) Since $2^3 \equiv 8 \equiv 1 \pmod 7$. This means $2^n \pmod 7$ is periodic with period 3. It suffices to consider three cases

1. If $n = 3k$, then $2^n - 1 \equiv 2^{3k} - 1 \equiv (2^3)^k - 1 \equiv 1^k - 1 \equiv 1 - 1 \equiv 0 \pmod 7$.
2. If $n = 3k + 1$, then $2^n - 1 \equiv 2^{3k+1} - 1 \equiv 2 \times 2^{3k} - 1 \equiv 2 - 1 \equiv 1 \pmod 7$.
3. If $n = 3k + 2$, then $2^n - 1 \equiv 4 \times 2^{3k} - 1 \equiv 4 - 1 \equiv 3 \pmod 7$.
4. Therefore, we conclude that $2^n - 1$ is divisible by 7 if and only if $n = 3k$, that is $n \equiv 0 \pmod 3$.
5. The proof of (b) is similar to (a) and will be left as exercise for the audience.

□

## Example (IMO 1964 Q1)

*(a) Find all natural numbers $n$ for which 7 divides $2^n - 1$.*
*(b) Prove that there is no natural number $n$ for which 7 divides $2^n + 1$.*

## Proof.

(a) Since $2^3 \equiv 8 \equiv 1 \pmod 7$. This means $2^n \pmod 7$ is periodic with period 3. It suffices to consider three cases

1. If $n = 3k$, then $2^n - 1 \equiv 2^{3k} - 1 \equiv (2^3)^k - 1 \equiv 1^k - 1 \equiv 1 - 1 \equiv 0 \pmod 7$.
2. If $n = 3k + 1$, then $2^n - 1 \equiv 2^{3k+1} - 1 \equiv 2 \times 2^{3k} - 1 \equiv 2 - 1 \equiv 1 \pmod 7$.
3. If $n = 3k + 2$, then $2^n - 1 \equiv 4 \times 2^{3k} - 1 \equiv 4 - 1 \equiv 3 \pmod 7$.
4. Therefore, we conclude that $2^n - 1$ is divisible by 7 if and only if $n = 3k$, that is $n \equiv 0 \pmod 3$.
5. The proof of (b) is similar to (a) and will be left as exercise for the audience.

□

## Example (IMO 1964 Q1)

*(a) Find all natural numbers $n$ for which 7 divides $2^n - 1$.*
*(b) Prove that there is no natural number $n$ for which 7 divides $2^n + 1$.*

## Proof.

(a) Since $2^3 \equiv 8 \equiv 1 \pmod 7$. This means $2^n \pmod 7$ is periodic with period 3. It suffices to consider three cases

1. If $n = 3k$, then $2^n - 1 \equiv 2^{3k} - 1 \equiv (2^3)^k - 1 \equiv 1^k - 1 \equiv 1 - 1 \equiv 0 \pmod 7$.
2. If $n = 3k + 1$, then $2^n - 1 \equiv 2^{3k+1} - 1 \equiv 2 \times 2^{3k} - 1 \equiv 2 - 1 \equiv 1 \pmod 7$.
3. If $n = 3k + 2$, then $2^n - 1 \equiv 4 \times 2^{3k} - 1 \equiv 4 - 1 \equiv 3 \pmod 7$.
4. Therefore, we conclude that $2^n - 1$ is divisible by 7 if and only if $n = 3k$, that is $n \equiv 0 \pmod 3$.
5. The proof of (b) is similar to (a) and will be left as exercise for the audience.

□

### Example (IMO 1964 Q1)

*(a) Find all natural numbers $n$ for which 7 divides $2^n - 1$.*
*(b) Prove that there is no natural number $n$ for which 7 divides $2^n + 1$.*

### Proof.

(a) Since $2^3 \equiv 8 \equiv 1 \pmod 7$. This means $2^n \pmod 7$ is periodic with period 3. It suffices to consider three cases

1. If $n = 3k$, then $2^n - 1 \equiv 2^{3k} - 1 \equiv (2^3)^k - 1 \equiv 1^k - 1 \equiv 1 - 1 \equiv 0 \pmod 7$.
2. If $n = 3k + 1$, then $2^n - 1 \equiv 2^{3k+1} - 1 \equiv 2 \times 2^{3k} - 1 \equiv 2 - 1 \equiv 1 \pmod 7$.
3. If $n = 3k + 2$, then $2^n - 1 \equiv 4 \times 2^{3k} - 1 \equiv 4 - 1 \equiv 3 \pmod 7$.
4. Therefore, we conclude that $2^n - 1$ is divisible by 7 if and only if $n = 3k$, that is $n \equiv 0 \pmod 3$.
5. The proof of (b) is similar to (a) and will be left as exercise for the audience.

□

## Example (IMO 1964 Q1)

*(a) Find all natural numbers $n$ for which 7 divides $2^n - 1$.*
*(b) Prove that there is no natural number $n$ for which 7 divides $2^n + 1$.*

## Proof.

(a) Since $2^3 \equiv 8 \equiv 1 \pmod 7$. This means $2^n \pmod 7$ is periodic with period 3. It suffices to consider three cases

1. If $n = 3k$, then $2^n - 1 \equiv 2^{3k} - 1 \equiv (2^3)^k - 1 \equiv 1^k - 1 \equiv 1 - 1 \equiv 0 \pmod 7$.
2. If $n = 3k + 1$, then $2^n - 1 \equiv 2^{3k+1} - 1 \equiv 2 \times 2^{3k} - 1 \equiv 2 - 1 \equiv 1 \pmod 7$.
3. If $n = 3k + 2$, then $2^n - 1 \equiv 4 \times 2^{3k} - 1 \equiv 4 - 1 \equiv 3 \pmod 7$.
4. Therefore, we conclude that $2^n - 1$ is divisible by 7 if and only if $n = 3k$, that is $n \equiv 0 \pmod 3$.
5. The proof of (b) is similar to (a) and will be left as exercise for the audience.

□

## Example (IMO 1964 Q1)

*(a) Find all natural numbers $n$ for which 7 divides $2^n - 1$.*
*(b) Prove that there is no natural number $n$ for which 7 divides $2^n + 1$.*

## Proof.

(a) Since $2^3 \equiv 8 \equiv 1 \pmod{7}$. This means $2^n \pmod{7}$ is periodic with period 3. It suffices to consider three cases

1. If $n = 3k$, then $2^n - 1 \equiv 2^{3k} - 1 \equiv (2^3)^k - 1 \equiv 1^k - 1 \equiv 1 - 1 \equiv 0 \pmod{7}$.
2. If $n = 3k+1$, then $2^n - 1 \equiv 2^{3k+1} - 1 \equiv 2 \times 2^{3k} - 1 \equiv 2 - 1 \equiv 1 \pmod{7}$.
3. If $n = 3k+2$, then $2^n - 1 \equiv 4 \times 2^{3k} - 1 \equiv 4 - 1 \equiv 3 \pmod{7}$.
4. Therefore, we conclude that $2^n - 1$ is divisible by 7 if and only if $n = 3k$, that is $n \equiv 0 \pmod{3}$.
5. The proof of (b) is similar to (a) and will be left as exercise for the audience.

□

## Example (HKIMO Prelim Shortlist)

$$\begin{aligned} a_1y + a_2z + a_3w &= 0 \\ a_4x + a_5z + a_6w &= 0 \\ a_7x + a_8y + a_9w &= 0 \\ a_{10}x + a_{11}y + a_{12}z &= 0, \end{aligned}$$

*where* $a_i \in \{1, -1\}$ *for* $1 \leq i \leq 12$. *Find the probability that* $(x, y, z, w) = (0, 0, 0, 0)$ *is the* $\boxed{\textit{only}}$ *solution to the system.*

## Idea.

It suffices to determine the probability that the matrix

$$A = \begin{pmatrix} 0 & a_1 & a_2 & a_3 \\ a_4 & 0 & a_5 & a_6 \\ a_7 & a_8 & 0 & a_9 \\ a_{10} & a_{11} & a_{12} & 0 \end{pmatrix}, \quad a_i \in \{1, -1\}$$

is invertible. i.e. $\det(A) \neq 0$. □

**Idea.**

I am going to first deal with a special case and then reduce the general case to this special case. □

**Special Case.**

Suppose $a_i = 1$ for all $i$, then the system has only the trivial solution because

$$\det \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} = -3 \neq 0.$$

□

**Reducing the general case to the special case.**

Now, since $-1 \equiv 1 \pmod 2$. We have

$$\begin{pmatrix} 0 & a_1 & a_2 & a_3 \\ a_4 & 0 & a_5 & a_6 \\ a_7 & a_8 & 0 & a_9 \\ a_{10} & a_{11} & a_{12} & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \pmod 2.$$

Therefore, we have:

$$\det \begin{pmatrix} 0 & a_1 & a_2 & a_3 \\ a_4 & 0 & a_5 & a_6 \\ a_7 & a_8 & 0 & a_9 \\ a_{10} & a_{11} & a_{12} & 0 \end{pmatrix} \equiv \det \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \equiv -3 \equiv 1 \pmod 2,$$

which is odd, and hence non-zero. Therefore, the system always has only the trivial solution for all choices of $a_i$. Hence the probability is 1. □

**Example (HKIMO 2009 Selection Test 1)**

*Find the total number of solutions to the following system of equations:*

$$
\begin{aligned}
a^2 + bc &\equiv a \pmod{37} \\
b(a+d) &\equiv b \pmod{37} \\
c(a+d) &\equiv c \pmod{37} \\
bc + d^2 &\equiv d \pmod{37} \\
ad - bc &\equiv 1 \pmod{37}
\end{aligned}
$$

**Proof.**

1. Let
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$
2. Then the first 4 equations of the system system is equivalent to $\boxed{A^2 \equiv A \pmod{37}}$,
3. and the last equation means the matrix $\boxed{A \text{ is invertible}}$.
4. This gives $A = I$ immediately. Hence the solution is unique.

$\square$

Proof.

1. Let
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$
2. Then the first 4 equations of the system system is equivalent to $\boxed{A^2 \equiv A \pmod{37}}$,
3. and the last equation means the matrix $\boxed{A \text{ is invertible}}$.
4. This gives $A = I$ immediately. Hence the solution is unique.

□

**Proof.**

1. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

2. Then the first 4 equations of the system system is equivalent to $\boxed{A^2 \equiv A \pmod{37}}$,
3. and the last equation means the matrix $\boxed{A \text{ is invertible}}$.
4. This gives $A = I$ immediately. Hence the solution is unique.

□

**Proof.**

1. Let
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$
2. Then the first 4 equations of the system system is equivalent to $\boxed{A^2 \equiv A \pmod{37}}$,
3. and the last equation means the matrix $\boxed{A \text{ is invertible}}$.
4. This gives $A = I$ immediately. Hence the solution is unique.

$\square$

*Proof.*

1. Let
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$
2. Then the first 4 equations of the system system is equivalent to $\boxed{A^2 \equiv A \pmod{37}}$,
3. and the last equation means the matrix $\boxed{A \text{ is invertible}}$.
4. This gives $A = I$ immediately. Hence the solution is unique.

$\square$

**Theorem (Fermat's Little Theorem)**

*Let $p$ be a prime, then we have*

$$a^p \equiv a \pmod{p} \quad \textit{for all} \quad a \geq 0.$$

**Proof.**

Fix a prime $p$, we proceed by induction on $a$.

1. For $a = 0$, we have $0^p - 0 \equiv 0 \pmod{p}$.
2. Assume $a^p \equiv a \pmod{p}$ some $a > 0$, we have

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \equiv a^p + 1 \pmod{p}.$$

   Note that $\binom{p}{k} \equiv 0 \pmod{p}$ for $1 \leq k \leq p-1$.
3. Hence $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$ by the induction hypothesis.
4. Therefore $S(a+1)$ is true and we are done by induction.

□

**Theorem (Fermat's Little Theorem)**

*Let p be a prime, then we have*

$$a^p \equiv a \pmod p \quad \textit{for all} \quad a \geq 0.$$

**Proof.**

Fix a prime $p$, we proceed by induction on $a$.

1. For $a = 0$, we have $0^p - 0 \equiv 0 \pmod p$.
2. Assume $a^p \equiv a \pmod p$ some $a > 0$, we have
$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \equiv a^p + 1 \pmod p.$$
Note that $\binom{p}{k} \equiv 0 \pmod p$ for $1 \leq k \leq p-1$.
3. Hence $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod p$ by the induction hypothesis.
4. Therefore $S(a+1)$ is true and we are done by induction.

□

**Theorem (Fermat's Little Theorem)**

*Let p be a prime, then we have*

$$a^p \equiv a \pmod{p} \quad \textit{for all} \quad a \geq 0.$$

**Proof.**

Fix a prime $p$, we proceed by induction on $a$.

1. For $a = 0$, we have $0^p - 0 \equiv 0 \pmod{p}$.
2. Assume $a^p \equiv a \pmod{p}$ some $a > 0$, we have

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \equiv a^p + 1 \pmod{p}.$$

   Note that $\binom{p}{k} \equiv 0 \pmod{p}$ for $1 \leq k \leq p-1$.
3. Hence $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$ by the induction hypothesis.
4. Therefore $S(a+1)$ is true and we are done by induction.

□

# Fermat's Little Theorem

## Theorem (Fermat's Little Theorem)

*Let p be a prime, then we have*

$$a^p \equiv a \pmod{p} \quad \textit{for all} \quad a \geq 0.$$

## Proof.

Fix a prime $p$, we proceed by induction on $a$.

1. For $a = 0$, we have $0^p - 0 \equiv 0 \pmod{p}$.
2. Assume $a^p \equiv a \pmod{p}$ some $a > 0$, we have

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \equiv a^p + 1 \pmod{p}.$$

   Note that $\binom{p}{k} \equiv 0 \pmod{p}$ for $1 \leq k \leq p-1$.

3. Hence $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$ by the induction hypothesis.
4. Therefore $S(a+1)$ is true and we are done by induction.

□

**Theorem (Fermat's Little Theorem)**

*Let $p$ be a prime, then we have*

$$a^p \equiv a \pmod{p} \quad \textit{for all} \quad a \geq 0.$$

**Proof.**

Fix a prime $p$, we proceed by induction on $a$.

1. For $a = 0$, we have $0^p - 0 \equiv 0 \pmod{p}$.
2. Assume $a^p \equiv a \pmod{p}$ some $a > 0$, we have

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \equiv a^p + 1 \pmod{p}.$$

   Note that $\binom{p}{k} \equiv 0 \pmod{p}$ for $1 \leq k \leq p-1$.
3. Hence $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$ by the induction hypothesis.
4. Therefore $S(a+1)$ is true and we are done by induction.

□

**Theorem**

*Let p be a prime, then we have*

$$(a+b)^p \equiv a^p + b^p \pmod{p} \quad \text{for all} \quad a, b \in \mathbb{Z}$$

**Proof.**

1. By Fermat's little theorem, we have $\boxed{a^p \equiv a \pmod{p},}$ and
2. $\boxed{b^p \equiv b \pmod{p}.}$
3. By Fermat's little theorem again, we have $(a+b)^p \equiv a+b \equiv a^p + b^p \pmod{p}$. Done.

□

**Theorem**

*Let $p$ be a prime, then we have*

$$(a+b)^p \equiv a^p + b^p \pmod{p} \quad \textit{for all} \quad a, b \in \mathbb{Z}$$

**Proof.**

1. By Fermat's little theorem, we have $\boxed{a^p \equiv a \pmod{p},}$ and
2. $\boxed{b^p \equiv b \pmod{p}.}$
3. By Fermat's little theorem again, we have $(a+b)^p \equiv a + b \equiv a^p + b^p \pmod{p}$. Done.

$\square$

**Theorem**

*Let $p$ be a prime, then we have*

$$(a+b)^p \equiv a^p + b^p \pmod{p} \quad \textit{for all} \quad a, b \in \mathbb{Z}$$

**Proof.**

1. By Fermat's little theorem, we have $\boxed{a^p \equiv a \pmod{p},}$ and
2. $\boxed{b^p \equiv b \pmod{p}.}$
3. By Fermat's little theorem again, we have $(a+b)^p \equiv a+b \equiv a^p + b^p \pmod{p}$. Done.

$\square$

**Theorem**

*Let p be a prime, then we have*

$$(a+b)^p \equiv a^p + b^p \pmod{p} \quad \textit{for all} \quad a, b \in \mathbb{Z}$$

**Proof.**

1. By Fermat's little theorem, we have $\boxed{a^p \equiv a \pmod{p},}$ and
2. $\boxed{b^p \equiv b \pmod{p}.}$
3. By Fermat's little theorem again, we have $(a+b)^p \equiv a+b \equiv a^p + b^p \pmod{p}$. Done.

□

**Example (HKIMO 2008 Prelim Q20)**

*For* $(1+x)^{38} = a_0 + a_1x + \ldots + a_{38}x^{38}$. *Let* $N_1 = \#\{a_i \mid a_i \equiv 1 \pmod 3\}$, $N_2 = \#\{a_i \mid a_i \equiv 2 \pmod 3\}$. *Compute* $N_1 - N_2$.

**Understanding the problem by trying a few small cases.**

1. First of all, we notice that we are only interested in the coefficients mod 3 and we therefore look at $(1+x)^n$ mod 3.
2. For $n = 3$, $(1+x)^3 \equiv 1 + x^3 \pmod 3$. That means $N_1 = 2$ and $N_2 = 0$.
3. For $n = 9$, $(1+x)^9 \equiv (1+x^3)^3 \equiv 1 + (x^3)^3 \equiv 1 + x^9 \pmod 3$. That means $N_1 = 2$ and $N_2 = 0$.
4. $(1+x)^{10} \equiv (1+x)(1+x)^9 \equiv (1+x)(1+x^9) \equiv 1 + x + x^9 + x^{10} \pmod 3$. That means $N_1 = 4$ and $N_2 = 0$.

□

## Example (HKIMO 2008 Prelim Q20)

*For* $(1+x)^{38} = a_0 + a_1 x + \ldots + a_{38}x^{38}$*. Let* $N_1 = \#\{a_i \mid a_i \equiv 1 \pmod 3\}$, $N_2 = \#\{a_i \mid a_i \equiv 2 \pmod 3\}$*. Compute* $N_1 - N_2$*.*

## Understanding the problem by trying a few small cases.

1. First of all, we notice that we are only interested in the coefficients mod 3 and we therefore look at $(1+x)^n$ mod 3.
2. For $n = 3$, $(1+x)^3 \equiv 1 + x^3 \pmod 3$. That means $N_1 = 2$ and $N_2 = 0$.
3. For $n = 9$, $(1+x)^9 \equiv (1+x^3)^3 \equiv 1 + (x^3)^3 \equiv 1 + x^9 \pmod 3$. That means $N_1 = 2$ and $N_2 = 0$.
4. $(1+x)^{10} \equiv (1+x)(1+x)^9 \equiv (1+x)(1+x^9) \equiv 1 + x + x^9 + x^{10} \pmod 3$. That means $N_1 = 4$ and $N_2 = 0$.

□

## Example (HKIMO 2008 Prelim Q20)

*For* $(1+x)^{38} = a_0 + a_1 x + \ldots + a_{38} x^{38}$. *Let* $N_1 = \#\{a_i \mid a_i \equiv 1 \pmod 3\}$, $N_2 = \#\{a_i \mid a_i \equiv 2 \pmod 3\}$. *Compute* $N_1 - N_2$.

## Understanding the problem by trying a few small cases.

1. First of all, we notice that we are only interested in the coefficients mod 3 and we therefore look at $(1+x)^n$ mod 3.
2. For $n = 3$, $(1+x)^3 \equiv 1 + x^3 \pmod 3$. That means $N_1 = 2$ and $N_2 = 0$.
3. For $n = 9$, $(1+x)^9 \equiv (1+x^3)^3 \equiv 1 + (x^3)^3 \equiv 1 + x^9 \pmod 3$. That means $N_1 = 2$ and $N_2 = 0$.
4. $(1+x)^{10} \equiv (1+x)(1+x)^9 \equiv (1+x)(1+x^9) \equiv 1 + x + x^9 + x^{10} \pmod 3$. That means $N_1 = 4$ and $N_2 = 0$.

□

**Example (HKIMO 2008 Prelim Q20)**

*For* $(1+x)^{38} = a_0 + a_1x + \ldots + a_{38}x^{38}$. *Let* $N_1 = \#\{a_i \mid a_i \equiv 1 \pmod 3\}$, $N_2 = \#\{a_i \mid a_i \equiv 2 \pmod 3\}$. *Compute* $N_1 - N_2$.

**Understanding the problem by trying a few small cases.**

1. First of all, we notice that we are only interested in the coefficients mod 3 and we therefore look at $(1+x)^n$ mod 3.
2. For $n = 3$, $(1+x)^3 \equiv 1 + x^3 \pmod 3$. That means $N_1 = 2$ and $N_2 = 0$.
3. For $n = 9$, $(1+x)^9 \equiv (1+x^3)^3 \equiv 1 + (x^3)^3 \equiv 1 + x^9 \pmod 3$. That means $N_1 = 2$ and $N_2 = 0$.
4. $(1+x)^{10} \equiv (1+x)(1+x)^9 \equiv (1+x)(1+x^9) \equiv 1 + x + x^9 + x^{10} \pmod 3$. That means $N_1 = 4$ and $N_2 = 0$.

□

### Example (HKIMO 2008 Prelim Q20)

*For* $(1+x)^{38} = a_0 + a_1 x + \ldots + a_{38}x^{38}$. *Let* $N_1 = \#\{a_i \mid a_i \equiv 1 \pmod 3\}$, $N_2 = \#\{a_i \mid a_i \equiv 2 \pmod 3\}$. *Compute* $N_1 - N_2$.

### Understanding the problem by trying a few small cases.

1. First of all, we notice that we are only interested in the coefficients mod 3 and we therefore look at $(1+x)^n$ mod 3.
2. For $n = 3$, $(1+x)^3 \equiv 1 + x^3 \pmod 3$. That means $N_1 = 2$ and $N_2 = 0$.
3. For $n = 9$, $(1+x)^9 \equiv (1+x^3)^3 \equiv 1 + (x^3)^3 \equiv 1 + x^9 \pmod 3$. That means $N_1 = 2$ and $N_2 = 0$.
4. $(1+x)^{10} \equiv (1+x)(1+x)^9 \equiv (1+x)(1+x^9) \equiv 1 + x + x^9 + x^{10}$ $\pmod 3$. That means $N_1 = 4$ and $N_2 = 0$.

□

**Idea.**

1. From the small cases, it seems writing 38 in base 3 should be fruitful.
2. The fact that $(a+b)^p \equiv a^p + b^p \pmod{p}$ should be the key.

□

**Proof.**

1. $38 = 27 + 9 + 2$.
2. $(1+x)^{p^k} \equiv 1 + x^{p^k} \pmod{p}$.
3. $(1+x)^{38} \equiv (1+x^{27})(1+x^9)(1+x)^2 \equiv (1+x^9)(1+x^{27})(1+2x+x^2) \pmod{3}$.
4. Therefore, we have $N_1 = 8$, $N_2 = 4$, and hence $N_1 - N_2 = 4$.

□

**Idea.**

1. From the small cases, it seems writing 38 in base 3 should be fruitful.
2. The fact that $(a+b)^p \equiv a^p + b^p \pmod{p}$ should be the key.

□

**Proof.**

1. $38 = 27 + 9 + 2$.
2. $(1+x)^{p^k} \equiv 1 + x^{p^k} \pmod{p}$.
3. $(1+x)^{38} \equiv (1+x^{27})(1+x^9)(1+x)^2 \equiv (1+x^9)(1+x^{27})(1+2x+x^2) \pmod{3}$.
4. Therefore, we have $N_1 = 8$, $N_2 = 4$, and hence $N_1 - N_2 = 4$.

□

**Idea.**

1. From the small cases, it seems writing 38 in base 3 should be fruitful.
2. The fact that $(a+b)^p \equiv a^p + b^p \pmod{p}$ should be the key.

□

**Proof.**

1. $38 = 27 + 9 + 2$.
2. $(1+x)^{p^k} \equiv 1 + x^{p^k} \pmod{p}$.
3. $(1+x)^{38} \equiv (1+x^{27})(1+x^9)(1+x)^2 \equiv (1+x^9)(1+x^{27})(1+2x+x^2) \pmod{3}$.
4. Therefore, we have $N_1 = 8$, $N_2 = 4$, and hence $N_1 - N_2 = 4$.

□

**Idea.**

1. From the small cases, it seems writing 38 in base 3 should be fruitful.
2. The fact that $(a+b)^p \equiv a^p + b^p \pmod{p}$ should be the key.

$\square$

**Proof.**

1. $38 = 27 + 9 + 2$.
2. $(1+x)^{p^k} \equiv 1 + x^{p^k} \pmod{p}$.
3. $(1+x)^{38} \equiv (1+x^{27})(1+x^9)(1+x)^2 \equiv (1+x^9)(1+x^{27})(1+2x+x^2) \pmod{3}$.
4. Therefore, we have $N_1 = 8$, $N_2 = 4$, and hence $N_1 - N_2 = 4$.

$\square$

**Idea.**

1. From the small cases, it seems writing 38 in base 3 should be fruitful.
2. The fact that $(a+b)^p \equiv a^p + b^p \pmod{p}$ should be the key.

□

**Proof.**

1. $38 = 27 + 9 + 2$.
2. $(1+x)^{p^k} \equiv 1 + x^{p^k} \pmod{p}$.
3. $(1+x)^{38} \equiv (1+x^{27})(1+x^9)(1+x)^2 \equiv (1+x^9)(1+x^{27})(1+2x+x^2) \pmod{3}$.
4. Therefore, we have $N_1 = 8$, $N_2 = 4$, and hence $N_1 - N_2 = 4$.

□

**Idea.**

1. From the small cases, it seems writing 38 in base 3 should be fruitful.
2. The fact that $(a+b)^p \equiv a^p + b^p \pmod{p}$ should be the key.

□

**Proof.**

1. $38 = 27 + 9 + 2$.
2. $(1+x)^{p^k} \equiv 1 + x^{p^k} \pmod{p}$.
3. $(1+x)^{38} \equiv (1+x^{27})(1+x^9)(1+x)^2 \equiv (1+x^9)(1+x^{27})(1+2x+x^2) \pmod{3}$.
4. Therefore, we have $N_1 = 8$, $N_2 = 4$, and hence $N_1 - N_2 = 4$.

□

**Idea.**

1. From the small cases, it seems writing 38 in base 3 should be fruitful.
2. The fact that $(a+b)^p \equiv a^p + b^p \pmod{p}$ should be the key.

□

**Proof.**

1. $38 = 27 + 9 + 2$.
2. $(1+x)^{p^k} \equiv 1 + x^{p^k} \pmod{p}$.
3. $(1+x)^{38} \equiv (1+x^{27})(1+x^9)(1+x)^2 \equiv (1+x^9)(1+x^{27})(1+2x+x^2) \pmod{3}$.
4. Therefore, we have $N_1 = 8$, $N_2 = 4$, and hence $N_1 - N_2 = 4$.

□

### Food for Thoughts

*What is the total number of odd coefficients in the* 100*th row of the Pascal Triangle?*
*[The first row and second row of the Pascal Triangle is* 1 1 *and* 1 2 1 *respectively.]*

### Food for Thoughts

*Suppose*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

*and let $p$ be a prime. What is the total number of solutions to $A^2 \equiv A \pmod{p}$?*

**Example (HKIMO 2009 Selection Test 1)**

*For the equation* $y^{37} = x^3 + 11$.
*Show that the equation is solvable mod* $p$ *for all primes* $p < 100$.

Before solving the problem, let me tell you how I came up with this problem.

1. Numbers 3 and 37 are completely artificial.
2. The number 11 serves the purpose to eliminate the possibility that there could be a trivial or simple-to-fine global solution. (i.e. an integer solution to the equation)
3. I had the mindset to kill the people who like to brute force.
4. I like to give "false hope" to the students who like to brute force, and therefore the number "100" is chosen. (after all, there are only 25 primes to check.)
5. However, the brute-force-group should ran into trouble after a while (i.e. after the first 10 primes or so ... I mean, computing the 37th power of a number mod a prime p is really not that easy.)

**Example (HKIMO 2009 Selection Test 1)**

*For the equation* $y^{37} = x^3 + 11$.
*Show that the equation is solvable mod p for all primes* $p < 100$.

Before solving the problem, let me tell you how I came up with this problem.

1. Numbers 3 and 37 are completely artificial.
2. The number 11 serves the purpose to eliminate the possibility that there could be a trivial or simple-to-fine global solution. (i.e. an integer solution to the equation)
3. I had the mindset to kill the people who like to brute force.
4. I like to give "false hope" to the students who like to brute force, and therefore the number "100" is chosen. (after all, there are only 25 primes to check.)
5. However, the brute-force-group should ran into trouble after a while (i.e. after the first 10 primes or so ... I mean, computing the 37th power of a number mod a prime p is really not that easy.)

**Example (HKIMO 2009 Selection Test 1)**

*For the equation* $y^{37} = x^3 + 11$.
*Show that the equation is solvable mod p for all primes* $p < 100$.

Before solving the problem, let me tell you how I came up with this problem.

1. Numbers 3 and 37 are completely artificial.
2. The number 11 serves the purpose to eliminate the possibility that there could be a trivial or simple-to-fine global solution. (i.e. an integer solution to the equation)
3. I had the mindset to kill the people who like to brute force.
4. I like to give "false hope" to the students who like to brute force, and therefore the number "100" is chosen. (after all, there are only 25 primes to check.)
5. However, the brute-force-group should ran into trouble after a while (i.e. after the first 10 primes or so ... I mean, computing the 37th power of a number mod a prime p is really not that easy.)

**Example (HKIMO 2009 Selection Test 1)**

*For the equation* $y^{37} = x^3 + 11$.
*Show that the equation is solvable mod* $p$ *for all primes* $p < 100$.

Before solving the problem, let me tell you how I came up with this problem.

1. Numbers 3 and 37 are completely artificial.
2. The number 11 serves the purpose to eliminate the possibility that there could be a trivial or simple-to-fine global solution. (i.e. an integer solution to the equation)
3. I had the mindset to kill the people who like to brute force.
4. I like to give "false hope" to the students who like to brute force, and therefore the number "100" is chosen. (after all, there are only 25 primes to check.)
5. However, the brute-force-group should ran into trouble after a while (i.e. after the first 10 primes or so ... I mean, computing the 37th power of a number mod a prime p is really not that easy.)

### Example (HKIMO 2009 Selection Test 1)

*For the equation* $y^{37} = x^3 + 11$.
*Show that the equation is solvable mod p for all primes* $p < 100$.

Before solving the problem, let me tell you how I came up with this problem.

1. Numbers 3 and 37 are completely artificial.
2. The number 11 serves the purpose to eliminate the possibility that there could be a trivial or simple-to-fine global solution. (i.e. an integer solution to the equation)
3. I had the mindset to kill the people who like to brute force.
4. I like to give "false hope" to the students who like to brute force, and therefore the number "100" is chosen. (after all, there are only 25 primes to check.)
5. However, the brute-force-group should ran into trouble after a while (i.e. after the first 10 primes or so ... I mean, computing the 37th power of a number mod a prime p is really not that easy.)

**Example (HKIMO 2009 Selection Test 1)**

*For the equation* $y^{37} = x^3 + 11$.
*Show that the equation is solvable mod* $p$ *for all primes* $p < 100$.

Before solving the problem, let me tell you how I came up with this problem.

1. Numbers 3 and 37 are completely artificial.
2. The number 11 serves the purpose to eliminate the possibility that there could be a trivial or simple-to-fine global solution. (i.e. an integer solution to the equation)
3. I had the mindset to kill the people who like to brute force.
4. I like to give "false hope" to the students who like to brute force, and therefore the number "100" is chosen. (after all, there are only 25 primes to check.)
5. However, the brute-force-group should ran into trouble after a while (i.e. after the first 10 primes or so . . . I mean, computing the 37th power of a number mod a prime p is really not that easy.)

**Theorem ($q$-th power lemma)**

*Suppose $p$ and $q$ are primes. Then every integer $a$ is a $q$th power mod $p$ if* $\gcd(p-1,q)=1$.
*In other words, if* $\gcd(p-1,q)=1$*, then the equation* $x^q \equiv a \pmod{p}$ *is solvable for all* $a$.

**Example**

*Since* $\gcd(5-1,3)=1$. *Every integer is a cube mod* 5.
*Indeed,*

$$1^3 \equiv 1 \pmod{5},$$
$$2^3 \equiv 8 \equiv 3 \pmod{5},$$
$$3^3 \equiv (-2)^3 \equiv -8 \equiv 2 \pmod{5}.$$
$$4^3 \equiv (-1)^3 \equiv -4 \equiv 4 \pmod{5}$$

Back to our problem

### Example

*For the equation* $y^{37} = x^3 + 11$.
*Show that the equation is solvable mod* $p$ *for all primes* $p < 100$.

### Proof.

1. If $(p-1, 3) = 1$ or $(p-1, 37) = 1$,
2. then the cubing lemma and the 37th power lemma says the equation is solvable since everything is either a cube or a 37th power.
3. Therefore, we only need to check primes $p$ such that

$$p \equiv 1 \pmod 3 \quad \text{and} \quad p \equiv 1 \pmod{37}.$$

4. i.e. $p \equiv 1 \pmod{111}$.
5. However, there is no such prime less than 100. We are done.

□

Back to our problem

**Example**

*For the equation* $y^{37} = x^3 + 11$.
*Show that the equation is solvable mod* $p$ *for all primes* $p < 100$.

**Proof.**

1. If $(p-1, 3) = 1$ or $(p-1, 37) = 1$,
2. then the cubing lemma and the 37th power lemma says the equation is solvable since everything is either a cube or a 37th power.
3. Therefore, we only need to check primes $p$ such that

$$p \equiv 1 \pmod 3 \quad \text{and} \quad p \equiv 1 \pmod{37}.$$

4. i.e. $p \equiv 1 \pmod{111}$.
5. However, there is no such prime less than 100. We are done.

□

Back to our problem

**Example**

*For the equation* $y^{37} = x^3 + 11$.
*Show that the equation is solvable mod* $p$ *for all primes* $p < 100$.

**Proof.**

1. If $(p-1, 3) = 1$ or $(p-1, 37) = 1$,
2. then the cubing lemma and the 37th power lemma says the equation is solvable since everything is either a cube or a 37th power.
3. Therefore, we only need to check primes $p$ such that

$$p \equiv 1 \pmod 3 \quad \text{and} \quad p \equiv 1 \pmod{37}.$$

4. i.e. $p \equiv 1 \pmod{111}$.
5. However, there is no such prime less than 100. We are done.

□

Back to our problem

**Example**

*For the equation* $y^{37} = x^3 + 11$.
*Show that the equation is solvable mod* $p$ *for all primes* $p < 100$.

**Proof.**

1. If $(p-1, 3) = 1$ or $(p-1, 37) = 1$,
2. then the cubing lemma and the 37th power lemma says the equation is solvable since everything is either a cube or a 37th power.
3. Therefore, we only need to check primes $p$ such that

$$p \equiv 1 \pmod 3 \quad \text{and} \quad p \equiv 1 \pmod{37}.$$

4. i.e. $p \equiv 1 \pmod{111}$.
5. However, there is no such prime less than 100. We are done.

□

Back to our problem

### Example

*For the equation* $y^{37} = x^3 + 11$.
*Show that the equation is solvable mod* $p$ *for all primes* $p < 100$.

### Proof.

1. If $(p-1,3) = 1$ or $(p-1,37) = 1$,
2. then the cubing lemma and the 37th power lemma says the equation is solvable since everything is either a cube or a 37th power.
3. Therefore, we only need to check primes $p$ such that

$$p \equiv 1 \pmod 3 \quad \text{and} \quad p \equiv 1 \pmod{37}.$$

4. i.e. $p \equiv 1 \pmod{111}$.
5. However, there is no such prime less than 100. We are done.

□

Back to our problem

**Example**

*For the equation* $y^{37} = x^3 + 11$.
*Show that the equation is solvable mod* $p$ *for all primes* $p < 100$.

**Proof.**

1. If $(p-1,3) = 1$ or $(p-1,37) = 1$,
2. then the cubing lemma and the 37th power lemma says the equation is solvable since everything is either a cube or a 37th power.
3. Therefore, we only need to check primes $p$ such that

$$p \equiv 1 \pmod 3 \quad \text{and} \quad p \equiv 1 \pmod{37}.$$

4. i.e. $p \equiv 1 \pmod{111}$.
5. However, there is no such prime less than 100. We are done.

□

**Theorem ($q$-th power lemma)**

*Suppose $p$ and $q$ are primes. Then every integer $a$ is a $q$th power mod $p$ if* $\gcd(p-1,q)=1$.
*In other words, if* $\gcd(p-1,q)=1$*, then the equation* $x^q \equiv a \pmod{p}$ *is solvable for all* $a$.

**Proof.**

1. Suppose $\gcd(p-1,q)=1$.
2. Then there exists integers $x$ and $y$ such that $x(p-1)+qy=1$.
3. Therefore,

$$a^1 \equiv a^{x(p-1)+qy} \equiv a^{p(x-1)} \times a^{qy} \equiv a^{qy}$$

   by Fermats little theorem.
4. Hence $a=(a^y)^q$ is a $q$-th power mod $p$ and we are done.

□

**Theorem ($q$-th power lemma)**

*Suppose p and q are primes. Then every integer a is a qth power mod p if* $\gcd(p-1, q) = 1$.
*In other words, if* $\gcd(p-1, q) = 1$, *then the equation* $x^q \equiv a \pmod{p}$ *is solvable for all a.*

**Proof.**

1. Suppose $\gcd(p-1, q) = 1$.
2. Then there exists integers $x$ and $y$ such that $x(p-1) + qy = 1$.
3. Therefore,
$$a^1 \equiv a^{x(p-1)+qy} \equiv a^{p(x-1)} \times a^{qy} \equiv a^{qy}$$
by Fermats little theorem.
4. Hence $a = (a^y)^q$ is a $q$-th power mod $p$ and we are done.

□

# Proof of the Cubing/$q$-th power Lemma

**Theorem ($q$-th power lemma)**

*Suppose $p$ and $q$ are primes. Then every integer $a$ is a $q$th power mod $p$ if* $\gcd(p-1, q) = 1$.
*In other words, if* $\gcd(p-1, q) = 1$, *then the equation* $x^q \equiv a \pmod{p}$ *is solvable for all* $a$.

**Proof.**

1. Suppose $\gcd(p-1, q) = 1$.
2. Then there exists integers $x$ and $y$ such that $x(p-1) + qy = 1$.
3. Therefore,
$$a^1 \equiv a^{x(p-1)+qy} \equiv a^{p(x-1)} \times a^{qy} \equiv a^{qy}$$
by Fermats little theorem.
4. Hence $a = (a^y)^q$ is a $q$-th power mod $p$ and we are done.

□

**Theorem ($q$-th power lemma)**

*Suppose $p$ and $q$ are primes. Then every integer $a$ is a $q$th power mod $p$ if* $\gcd(p-1, q) = 1$.
*In other words, if* $\gcd(p-1, q) = 1$, *then the equation* $x^q \equiv a \pmod{p}$ *is solvable for all $a$.*

**Proof.**

1. Suppose $\gcd(p-1, q) = 1$.
2. Then there exists integers $x$ and $y$ such that $x(p-1) + qy = 1$.
3. Therefore,
$$a^1 \equiv a^{x(p-1)+qy} \equiv a^{p(x-1)} \times a^{qy} \equiv a^{qy}$$
by Fermats little theorem.
4. Hence $a = (a^y)^q$ is a $q$-th power mod $p$ and we are done.

□

**Theorem ($q$-th power lemma)**

*Suppose $p$ and $q$ are primes. Then every integer $a$ is a $q$th power mod $p$ if $\gcd(p-1, q) = 1$.*
*In other words, if $\gcd(p-1, q) = 1$, then the equation $x^q \equiv a \pmod{p}$ is solvable for all $a$.*

**Proof.**

1. Suppose $\gcd(p-1, q) = 1$.
2. Then there exists integers $x$ and $y$ such that $x(p-1) + qy = 1$.
3. Therefore,
$$a^1 \equiv a^{x(p-1)+qy} \equiv a^{p(x-1)} \times a^{qy} \equiv a^{qy}$$
by Fermats little theorem.
4. Hence $a = (a^y)^q$ is a $q$-th power mod $p$ and we are done.

□

**Question**

*Is it possible to find infinitely many primes that ends in 2010?*

**Answer.**

1. NO...
2. You cannot even find one prime that ends in 2010.

□

**Question**

*Is it possible to find infinitely many primes that ends in 2011?*
*[Note that 2011 is a prime number.]*

**Question**

*Is it possible to find infinitely many primes that ends in 123?*

**Question**

*Is it possible to find infinitely many primes that ends in 2010?*

**Answer.**

1. NO...
2. You cannot even find one prime that ends in 2010.

□

**Question**

*Is it possible to find infinitely many primes that ends in 2011?*
*[Note that 2011 is a prime number.]*

**Question**

*Is it possible to find infinitely many primes that ends in 123?*

**Question**

*Is it possible to find infinitely many primes that ends in 2010?*

**Answer.**

1. NO...
2. You cannot even find one prime that ends in 2010.

□

**Question**

*Is it possible to find infinitely many primes that ends in 2011?*
*[Note that 2011 is a prime number.]*

**Question**

*Is it possible to find infinitely many primes that ends in 123?*

The answer is YES due to the following theorem.

**Theorem (Dirichlet)**

*Suppose $k$ and $a$ are integers that are relatively prime. Then the sequence $\{kn + a\}$ contains infinitely many primes. In other words, there are infinitely many primes such that $p \equiv a \pmod{k}$.*

**Solution.**

1. Let $k = 10^4$ and $a = 2011$, then $\gcd(k, a) = 1$.
2. By Dirichlet's theorem, we have the sequence $\{10000n + 2011\}$ contains infinitely many primes.
3. Likewise, since $\gcd(1000, 123) = 1$, Dirichlet's theorem says $\{1000n + 123\}$ contains infinitely many primes.

□

By a similar argument, we have the following theorem

**Theorem**

*Given any integer $a$ such that $\gcd(a, 10) = 1$, then there are infinitely many primes $p$ that ends in $a$.*

The answer is YES due to the following theorem.

**Theorem (Dirichlet)**

*Suppose $k$ and $a$ are integers that are relatively prime. Then the sequence $\{kn + a\}$ contains infinitely many primes. In other words, there are infinitely many primes such that $p \equiv a \pmod{k}$.*

**Solution.**

1. Let $k = 10^4$ and $a = 2011$, then $\gcd(k, a) = 1$.
2. By Dirichlet's theorem, we have the sequence $\{10000n + 2011\}$ contains infinitely many primes.
3. Likewise, since $\gcd(1000, 123) = 1$, Dirichlet's theorem says $\{1000n + 123\}$ contains infinitely many primes.

□

By a similar argument, we have the following theorem

**Theorem**

*Given any integer $a$ such that $\gcd(a, 10) = 1$, then there are infinitely many primes $p$ that ends in $a$.*

The answer is YES due to the following theorem.

**Theorem (Dirichlet)**

*Suppose $k$ and $a$ are integers that are relatively prime. Then the sequence $\{kn + a\}$ contains infinitely many primes. In other words, there are infinitely many primes such that $p \equiv a \pmod{k}$.*

**Solution.**

1. Let $k = 10^4$ and $a = 2011$, then $\gcd(k, a) = 1$.
2. By Dirichlet's theorem, we have the sequence $\{10000n + 2011\}$ contains infinitely many primes.
3. Likewise, since $\gcd(1000, 123) = 1$, Dirichlet's theorem says $\{1000n + 123\}$ contains infinitely many primes.

□

By a similar argument, we have the following theorem

**Theorem**

*Given any integer $a$ such that $\gcd(a, 10) = 1$, then there are infinitely many primes $p$ that ends in $a$.*

The answer is YES due to the following theorem.

**Theorem (Dirichlet)**

*Suppose $k$ and $a$ are integers that are relatively prime. Then the sequence $\{kn + a\}$ contains infinitely many primes. In other words, there are infinitely many primes such that $p \equiv a \pmod{k}$.*

**Solution.**

1. Let $k = 10^4$ and $a = 2011$, then $\gcd(k, a) = 1$.
2. By Dirichlet's theorem, we have the sequence $\{10000n + 2011\}$ contains infinitely many primes.
3. Likewise, since $\gcd(1000, 123) = 1$, Dirichlet's theorem says $\{1000n + 123\}$ contains infinitely many primes.

□

By a similar argument, we have the following theorem

**Theorem**

*Given any integer $a$ such that $\gcd(a, 10) = 1$, then there are infinitely many primes $p$ that ends in $a$.*

**Question**

*Given* $\gcd(k, a) = 1$. *If we randomly choose a prime number* $p$*, what is the probability that* $p \equiv a \pmod{k}$?

The answer is given by the following

**Theorem (Chebotarev's Density Theorem)**

*Given* $\gcd(k, a) = 1$. *If we randomly choose a prime number* $p$*, what is the probability that* $p \equiv a \pmod{k}$ *is* $\frac{1}{\varphi(k)}$.

### Question

*What is* $\varphi(k)$?

### Definition (Euler $\varphi$ function)

Let $\varphi(m) = \{$number of integers, $a$ less than $m$ and relatively prime to $m\}$. i.e. $\varphi(m) = \{a \in \mathbb{N} \,|\, (a, m) = 1 \text{ and } a < m.\}$.

### Example

1. $\varphi(4) = 2$, *since* $1, 3$ *are the integers less than* $4$ *and are relatively prime to* $4$.
2. $\varphi(5) = 4$, *viz.* $1, 2, 3, 4$ *are less than* $5$ *and are relatively prime to* $5$.
3. $\varphi(10) = 4$, *namely* $1, 3, 7, 9$ *are less than* $10$ *are are relatively prime to* $10$.

**Question**

*What is* $\varphi(k)$?

**Definition (Euler $\varphi$ function)**

Let $\varphi(m) = \{$number of integers, $a$ less than $m$ and relatively prime to $m\}$. i.e. $\varphi(m) = \{a \in \mathbb{N} \,|\, (a, m) = 1 \text{ and } a < m.\}$.

**Example**

1. $\varphi(4) = 2$, *since* $1, 3$ *are the integers less than* $4$ *and are relatively prime to* $4$.
2. $\varphi(5) = 4$, *viz.* $1, 2, 3, 4$ *are less than* $5$ *and are relatively prime to* $5$.
3. $\varphi(10) = 4$, *namely* $1, 3, 7, 9$ *are less than* $10$ *are are relatively prime to* $10$.

## Question

*What is $\varphi(k)$?*

## Definition (Euler $\varphi$ function)

Let $\varphi(m) = \{$number of integers, $a$ less than $m$ and relatively prime to $m\}$. i.e. $\varphi(m) = \{a \in \mathbb{N} \,|\, (a, m) = 1 \text{ and } a < m.\}$.

## Example

1. $\varphi(4) = 2$, *since* $1, 3$ *are the integers less than* $4$ *and are relatively prime to* $4$.
2. $\varphi(5) = 4$, *viz.* $1, 2, 3, 4$ *are less than* $5$ *and are relatively prime to* $5$.
3. $\varphi(10) = 4$, *namely* $1, 3, 7, 9$ *are less than* $10$ *are are relatively prime to* $10$.

### Question

*What is* $\varphi(k)$?

### Definition (Euler $\varphi$ function)

Let $\varphi(m) = \{$number of integers, $a$ less than $m$ and relatively prime to $m\}$. i.e. $\varphi(m) = \{a \in \mathbb{N} \mid (a, m) = 1 \text{ and } a < m.\}$.

### Example

1. $\varphi(4) = 2$, *since* $1, 3$ *are the integers less than* $4$ *and are relatively prime to* $4$.
2. $\varphi(5) = 4$, *viz.* $1, 2, 3, 4$ *are less than* $5$ *and are relatively prime to* $5$.
3. $\varphi(10) = 4$, *namely* $1, 3, 7, 9$ *are less than* $10$ *are are relatively prime to* $10$.

### Theorem (Formula for $\varphi(m)$)

*Let $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, where the $p_i$ are distinct prime factors of $m$ then:*

$$\varphi(m) = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = m\left(1 - \frac{1}{p_1}\right) \times \cdots \times \left(1 - \frac{1}{p_k}\right).$$

### Example

1. *Since* $1000 = 2^3 \times 5^3$, *we have* $\varphi(1000) = 1000 \times (1 - 1/2)(1 - 1/5) = 400$.
2. *Since* $10000 = 2^4 \times 5^4$, *we have* $\varphi(10000) = 10000 \times (1 - 1/2)(1 - 1/5) = 4000$.

This gives

### Theorem

*There are infinitely many primes $p$ that ends in* 123 *and among all the primes, the probability of choosing a prime that ends in* 123 *is* $\frac{1}{\varphi(1000)} = \frac{1}{400}$.

### Theorem (Formula for $\varphi(m)$)

*Let $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, where the $p_i$ are distinct prime factors of $m$ then:*

$$\varphi(m) = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = m\left(1 - \frac{1}{p_1}\right) \times \cdots \times \left(1 - \frac{1}{p_k}\right).$$

### Example

1. *Since* $1000 = 2^3 \times 5^3$, *we have* $\varphi(1000) = 1000 \times (1 - 1/2)(1 - 1/5) = 400$.
2. *Since* $10000 = 2^4 \times 5^4$, *we have* $\varphi(10000) = 10000 \times (1 - 1/2)(1 - 1/5) = 4000$.

This gives

### Theorem

*There are infinitely many primes $p$ that ends in* 123 *and among all the primes, the probability of choosing a prime that ends in* 123 *is* $\frac{1}{\varphi(1000)} = \frac{1}{400}$.

**Theorem (Formula for $\varphi(m)$)**

*Let $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, where the $p_i$ are distinct prime factors of $m$ then:*

$$\varphi(m) = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = m \left(1 - \frac{1}{p_1}\right) \times \cdots \times \left(1 - \frac{1}{p_k}\right).$$

**Example**

1. *Since* $1000 = 2^3 \times 5^3$, *we have* $\varphi(1000) = 1000 \times (1 - 1/2)(1 - 1/5) = 400$.
2. *Since* $10000 = 2^4 \times 5^4$, *we have* $\varphi(10000) = 10000 \times (1 - 1/2)(1 - 1/5) = 4000$.

This gives

**Theorem**

*There are infinitely many primes $p$ that ends in 123 and among all the primes, the probability of choosing a prime that ends in 123 is* $\frac{1}{\varphi(1000)} = \frac{1}{400}$.

**Theorem (Fermat's Last Theorem)**

*Suppose* $n \geq 3$*. If* $x, y, z$ *are integers and* $x^n + y^n = z^n$*, then* $xyz = 0$.

For the proof, we shall do it next time!

**Food for Thoughts**

*Find all integer solutions to* $3x^2 + 1 = 4y^3$.

# Thanks

I would like to thank the HKAGE (Hong Kong Academy for Gifted Education) for the invitation and thank you all for coming!