$n = 2k$ $\qquad n^2 = (2k)^2 = 4k^2$

$4 \mid n^2$

$n = 2k+1$ $\qquad n^2 = (2k+1)^2$

$= 4k^2 + 4k + 1$

$= 4(\underbrace{k^2 + k}) + 1$

$= 4\ell + 1$

$n^2 \bmod 4 = 1$

$\boxed{\text{Fermat's Last Theorem}}$

$a^n + b^n = c^n$ $\quad \gcd(a,b,c) > 1$

No $\quad n > 2$

$\boxed{\text{Fermat's Little Theorem}}$

Let a be an integer and p a prime number.
If $p \nmid a$, then

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

$a = 7 \quad p = 3$

$7^2 \equiv 1 \pmod{3}$

22(e) Find $8^{4060} \bmod 4057$

Lot of work

$$\begin{cases} 8^{4060} \equiv x \pmod{4057} \\ x \equiv 8^{4060} \pmod{4057} \end{cases}$$

AKS algorithm $\rightarrow$ Polynomial time

$\sqrt{4057} \approx 63 \qquad (50)^2 = 2500$

$(65)^2 = 4225$

$(64)^2$

4057 is a prime number.

$4057 \nmid 8$.

Using Fermat' Little Theorem.

$8^{4056} \equiv 1 \pmod{4057}$

$8^4 \cdot 8^{4056} \equiv 8^4 \pmod{4057}$

$8^{4060} \equiv 8^4 \pmod{4057}$

$8^4 = (64)(64)$

$= 4096$

$8^{4060} \equiv 4096 \pmod{4057}$

$4096 \equiv 39 \pmod{4057}$

$8^{4060} \equiv 39 \pmod{4057}$

Last two digits of 9^{821}

What is $9^{821} \pmod{100}$

$212 = 21(10) + 2$

$212 = 2(100) + 12$

$9^2 = 81 \equiv -19 \pmod{100}$

$9^{820} = (9^2)^{410} \equiv (-19)^{410} \pmod{100}$

$(-19)^2 \equiv (61) \bmod 100$

$((-19)^2)^{205} \equiv (61)^{205} \bmod 100$

$19^2 = 361$

5.1 Mathematical Induction

Prove that

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}, \quad n \geq 1$$

$\Downarrow$

Property $P(n)$

$P(1)$: $1 \stackrel{?}{=} \frac{1(1+1)}{2}$ ✓

$P(1)$ is true.

$P(2)$: LHS : $1+2 = 3$

RHS : $\frac{\cancel{2}(2+1)}{\cancel{2}} = 3$

$P(2)$ is true.

Assume $P(k)$ is true $k \geq 1$

Show $P(k+1)$ is also true.

Show that

$$\underbrace{1+2+3+\cdots+n=\frac{n(n+1)}{2}}_{P(n)}, \quad n \geq 1$$

① Basis Step

We show that $P(1)$ is true — as 1 is the first value of n for which $P(n)$ will be true.

LHS: 1

RHS: $\frac{1(1+1)}{2} = 1$

LHS = RHS. Hence $P(1)$ is true.

② Induction Step

Suppose $P(n)$ is true for some $n=k \geq 1$

$\therefore P(k)$ is true

$$\Rightarrow \boxed{1+2+3+\cdots+k=\frac{k(k+1)}{2}}$$

Show that $P(k+1)$ is also true.

$1+2+3+\cdots+(k+1) \stackrel{?}{=} \frac{(k+1)(k+2)}{2}$

$$\Rightarrow 1+2+3+\cdots+k+(k+1)$$
$$=\frac{k(k+1)}{2}+(k+1)$$
$$=(k+1)\left[\frac{k}{2}+1\right]$$
$$=(k+1)\left(\frac{k+2}{2}\right)$$
$$=\frac{(k+1)((k+1)+1)}{2}$$

$\therefore P(k+1)$ is true

Hence the statement is true for all $n \geq 1$ by induction.

Principle of Mathematical Induction

Show $P(n)$, $n \geq n_0$

① Basis Step : Show $P(n_0)$ is true.

② Induction step : Assume $P(k)$ is true for some $n = k \geq n_0$

Show that $P(k+1)$ is also true

$\Rightarrow P(n)$ is true for all $n \geq n_0$.

Q. Prove that for any integer $n \geq 1$, $\underbrace{2^{2n} - 1 \text{ is divisible by } 3}$.

$P(n)$: $2^{2n} - 1$ is divisible by 3 for $n \geq 1$, $n \in \mathbb{Z}$

① $P(1)$: $2^2 - 1$ is divisible by 3 ?

$2^2 - 1 = 4 - 1 = 3$ is divisible by 3.

Hence $P(1)$ is true.

② Assume $P(k)$ is true for some $k \geq 1$

$\therefore$ $2^{2k} - 1$ is divisible by 3.

$\underline{\underline{P(k+1)}}$: $2^{2(k+1)} - 1$ is divisible by 3 ?

$$
\begin{aligned}
2^{2(k+1)} - 1 &= 2^{2k+2} - 1 \\
&= 2^{2k} \cdot 2^2 - 1 \\
&= 4 \cdot 2^{2k} - 1 \longrightarrow \underbrace{2^{2k} - 1} + \underbrace{3 \cdot 2^{2k}} \\
&= 4 \cdot 2^{2k} - 1 + 4 - 4 \\
&= 4 \cdot 2^{2k} - 4 + 3 \\
&= 4(2^{2k} - 1) + 3
\end{aligned}
$$

As $2^{2k} - 1$ and 3 are divisible by 3, hence $4(2^{2k} - 1) + 3$ is also divisible by 3.

$\therefore$ $P(k+1)$ is also true.

$\therefore$ $P(n)$ is true for integers $n \geq 1$.

9(b) $\underbrace{2^n \geq \frac{1}{8}}_{P(n)}$ for all $n \geq -3$

① $P(-3)$: $2^{-3} \geq \frac{1}{8}$?

$\underline{LHS}$: $2^{-3} = \frac{1}{2^3} = \frac{1}{8}$

$\underline{RHS}$: $\frac{1}{8}$

LHS $\geq$ RHS. $\therefore P(-3)$ is true.

② Assume that $P(k)$ is true for $k \geq -3$.

$\therefore 2^k \geq \frac{1}{8}$

$P(k+1)$: $2^{k+1} \geq \frac{1}{8}$?

$2^k \cdot 2 \geq \frac{1}{8} \cdot 2$

$2^{k+1} \geq \frac{1}{4} \geq \frac{1}{8}$

$\therefore 2^{k+1} \geq \frac{1}{8}$

Hence $P(k+1)$ is also true.

$\therefore P(n)$ is true for all $n \geq -3$.

Principle of Strong Induction

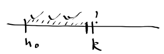
Statement $P(n)$, $n \geq n_0$

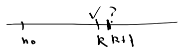
① **Basis Step** Show $P(n_0)$ is true

② **Inductive Step** Let $k > n_0$ be an integer st $P(l)$ is true for all $n_0 \leq l < k$.

Show that $P(k)$ is true.

Then $P(n)$ is true for all integers $n \geq n_0$.





---

① Prove that every integer $n \geq 2$ is either a prime or a product of prime numbers.

Strong Induction

① Basis Step: $P(2)$: 2 is either a prime or a product of primes?

As 2 is a prime, hence $P(2)$ is true.

② Inductive Step: Let $k > 2$, and let $P(l)$ be true for all $2 \leq l < k$.

$\therefore$ Every integer $2 \leq l < k$ is either a prime or a product of primes.

$P(k)$: k is a prime or a product of primes?

If k is a prime $\Rightarrow P(k)$ is true.

If k is composite $\Rightarrow k = ab$ for $a, b \geq 2$, $a, b < k$

By Inductive step,

$P(a)$ and $P(b)$ are true.

Hence $k = ab$ is a product of primes.

$\therefore P(k)$ is true.

Hence $P(n)$ is true for all $n \geq 2$.

5.2 Recursive Sequences

2, 7, 9, 12, . . .

1, 2, 3, 4, 5, . . .

A sequence is a function $f: \mathbb{N} \to \mathbb{R}$

$f(1)$ $f(2)$ $f(3)$ $f(4)$
$\downarrow$ $\downarrow$ $\downarrow$ $\downarrow$
2, 7, 9, 12, . . .

The n^{th} term of a sequence is denoted by a_n

$a_1 = 2$	$a_1 = 1$
$a_2 = 7$	$a_2 = 2$
$a_3 = 9$	$a_3 = 3$
$a_4 = 12$	$a_4 = 4$
$\vdots$	$\vdots$
$a_n = ?$	$\boxed{a_n = n}$

1, 3, 5, 7, 9, . . .

$a_n = 2n - 1, \quad n \geq 1$

$\boxed{a_{n+1} = a_n + 2}, \quad n \geq 1$ ← Recursive relation

$\boxed{a_1 = 1}$ ← Initial condition.

$a_2 = a_1 + 2$
$a_3 = a_2 + 2$
$a_4 = a_3 + 2$

$a_{n+1} = a_n + 2 \quad , \quad a_1 = 1$

$a_1 = 1$

$a_2 = a_1 + 2 = 1 + 2$

$a_3 = a_2 + 2 = (1+2) + 2 = 1+2+2$

$a_4 = a_3 + 2 = (1+2+2) + 2 = 1+2+2+2$

$a_5 = a_4 + 2 = (1+2+2+2) + 2 = 1+2+2+2+2$

$\vdots$

$a_n = 1 + \underbrace{2+2+2+\cdots+2}_{(n-1)\text{ terms}}$

$a_n = 1 + 2(n-1) = 2n-1$

Now we need to verify that $a_n = 2n-1$ is indeed correct.

We will use induction to verify that

$\underbrace{a_n = 2n-1}_{P(n)} \quad , \quad n \geq 1$

$1, 3, 5, 7, \ldots$

$\boxed{a_{n+1} = a_n + 2}, \quad n \geq 1$

① Basis step : LHS: $a_1 = 1$ ✓

RHS: $2(1) - 1 = 1$ ✓

Hence, $P(1)$ is true.

② Inductive step : Assume that $P(k)$ is true for some $k \geq 1$.

WTS

$a_{k+1} = 2(k+1) - 1$

$\therefore a_k = 2k - 1$

$a_{k+1} = a_k + 2$

$= (2k-1) + 2$

$= 2k+1$

$= 2k + 2 - 1$

$a_{k+1} = 2(k+1) - 1$

$\therefore P(k+1)$ is also true.

Hence $P(n)$: $a_n = 2n-1$ is true for all $n \geq 1$.

Some standard sequences

(1) Arithmetic Sequence

$$\boxed{a_{n+1} = a_n + d} \leftarrow \text{Common difference}$$

$$\underbrace{-5, -8, -11, -14, \ldots}$$

$a_1 = -5$

$d = -3$

$$\boxed{a_n = a_1 + (n-1)d}, \; n \geq 1 \quad \text{Check}$$

Series

Adding the terms of a sequence results in a series

Arithmetic Series

Sequence $\rightarrow a_{n+1} = a_n + d$

Series $\rightarrow a_1 + a_2 + a_3 + \cdots + a_n$

$$\underbrace{2+4+6+8+\cdots+200}$$

$$2+5+8+11+\cdots+26$$

$a_2 = a_1 + d$

$a_3 = a_1 + 2d$

$a_4 = a_1 + 3d$

$\vdots$

$$S_n = a_1 + a_2 + \cdots + a_n$$

$$= (a_1) + (a_1 + d) + (a_1 + 2d) + (a_1 + 3d) + \cdots + (a_1 + (n-1)d)$$

$$= \underbrace{(a_1 + a_1 + \cdots + a_1)}_{n \text{ terms}} + (d + 2d + 3d + \cdots + (n-1)d)$$

$$= na_1 + d(1 + 2 + 3 + \cdots + (n-1))$$

$$= na_1 + d\frac{(n-1)n}{2}$$

$$= \boxed{n\left[a_1 + \frac{d(n-1)}{2}\right]}$$

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

$$\underbrace{2+5+8+11+\cdots+}_{20 \text{ terms}}$$

$a_1 = 2$

$d = 3$

$n = 20$

$$S = 20\left[2 + \frac{3 \cdot 19}{2}\right]$$

$$= 20\left[\frac{4+57}{2}\right] = 10[61] = 610.$$

$d = 1 \quad n = n$

$a_1 = 1$

$$S = n\left[1 + \frac{n-1}{2}\right]$$

$$= n\left[\frac{n+1}{2}\right]$$

② Geometric Sequence

$2, 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots, \frac{1}{1024}$

$a_{n+1} = \frac{1}{2} a_n \quad , a_1 = 2$

In general, a geometric sequence has a "common ratio" denoted by r.

$a_{n+1} = a_n r$

$a_1 = a_1$
$a_2 = r a_1$
$a_3 = r a_2 = r(r a_1) = r^2 a_1$
$a_4 = r a_3 = r(r^2 a_1) = r^3 a_1$
$\vdots$

$\boxed{a_n = a_1 r^{n-1}}$ ← Prediction

$a_{k+1} = a_k(r)$
$= a_1 r^{k-1} \cdot r$
$= a_1 r^k$
$= a_1 r^{(k+1)-1}$

Geometric Series

$a_1, a_1 r, a_1 r^2, a_1 r^3, \ldots, a_1 r^{n-1}$

$S = a_1 + a_1 r + a_1 r^2 + \ldots + a_1 r^{n-1}$
$= a_1 (1 + r + r^2 + \ldots + r^{n-1})$

$\boxed{S = a_1 \left(\frac{1 - r^n}{1 - r} \right)} \quad r \neq 1$

$M = 1 + \cancel{r} + \cancel{r^2} + \ldots + \cancel{r^{n-1}}$
$rM = \cancel{r} + \cancel{r^2} + \ldots + \cancel{r^{n-1}} + r^n$

$M - rM = 1 - r^n$
$M(1-r) = 1 - r^n$
$M = \frac{1 - r^n}{1 - r}$