http://www.tkiryl.com/teaching/aa/review1.pdf

1. MATHEMATICAL INDUCTION

EXAMPLE 1: Prove that

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2} \tag{1.1}$$

for any integer $n \geq 1$.

Proof:

STEP 1: For n=1 (1.1) is true, since

$$1 = \frac{1(1+1)}{2}.$$

STEP 2: Suppose (1.1) is true for some $n = k \geq 1$, that is

$$1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}.$$

STEP 3: Prove that (1.1) is true for $n = k + 1$, that is

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

We have

$$1 + 2 + 3 + \ldots + k + (k+1) \stackrel{\textbf{ST.2}}{=} \frac{k(k+1)}{2} + (k+1) = (k+1)\left(\frac{k}{2} + 1\right) = \frac{(k+1)(k+2)}{2}. \blacksquare$$

EXAMPLE 2: Prove that

$$1 + 3 + 5 + \ldots + (2n-1) = n^2 \tag{1.2}$$

for any integer $n \geq 1$.

Proof:

STEP 1: For n=1 (1.2) is true, since $1 = 1^2$.

STEP 2: Suppose (1.2) is true for some $n = k \geq 1$, that is

$$1 + 3 + 5 + \ldots + (2k-1) = k^2.$$

STEP 3: Prove that (1.2) is true for $n = k + 1$, that is

$$1 + 3 + 5 + \ldots + (2k-1) + (2k+1) \stackrel{?}{=} (k+1)^2.$$

We have: $1 + 3 + 5 + \ldots + (2k-1) + (2k+1) \stackrel{\textbf{ST.2}}{=} k^2 + (2k+1) = (k+1)^2.$ $\blacksquare$

<u>EXAMPLE 3</u>: Prove that

$$n! \le n^n \tag{1.3}$$

for any integer $n \ge 1$.

<u>Proof</u>:

STEP 1: For n=1 (1.3) is true, since $1! = 1^1$.

STEP 2: Suppose (1.3) is true for some $n = k \ge 1$, that is $k! \le k^k$.

STEP 3: Prove that (1.3) is true for $n = k+1$, that is $(k+1)! \overset{?}{\le} (k+1)^{k+1}$. We have

$$(k+1)! = k! \cdot (k+1) \overset{\textbf{ST.2}}{\le} k^k \cdot (k+1) < (k+1)^k \cdot (k+1) = (k+1)^{k+1}. \blacksquare$$

<u>EXAMPLE 4</u>: Prove that

$$8 \mid 3^{2n} - 1 \tag{1.4}$$

for any integer $n \ge 0$.

<u>Proof</u>:

STEP 1: For n=0 (1.4) is true, since $8 \mid 3^0 - 1$.

STEP 2: Suppose (1.4) is true for some $n = k \ge 0$, that is $8 \mid 3^{2k} - 1$.

STEP 3: Prove that (1.4) is true for $n = k+1$, that is $8 \mid 3^{2(k+1)} - 1$. We have

$$3^{2(k+1)} - 1 = 3^{2k+2} - 1 = 3^{2k} \cdot 9 - 1 = 3^{2k}(8+1) - 1 = \underbrace{3^{2k} \cdot 8}_{\text{div. by } 8} + \underbrace{3^{2k} - 1}_{\substack{\text{St. 2} \\ \text{div. by } 8}}. \blacksquare$$

<u>EXAMPLE 5</u>: Prove that

$$7 \mid n^7 - n \tag{1.5}$$

for any integer $n \ge 1$.

<u>Proof</u>:

STEP 1: For n=1 (1.5) is true, since $7 \mid 1^7 - 1$.

STEP 2: Suppose (1.5) is true for some $n = k \ge 1$, that is

$$7 \mid k^7 - k.$$

STEP 3: Prove that (1.5) is true for $n = k+1$, that is $7 \mid (k+1)^7 - (k+1)$. We have

$$\begin{aligned}(k+1)^7 - (k+1) &= k^7 + 7k^6 + 21k^5 + 35k^4 + 35k^3 + 21k^2 + 7k + 1 - k - 1 \\ &= \underbrace{k^7 - k}_{\substack{\text{St. 2} \\ \text{div. by } 7}} + \underbrace{7k^6 + 21k^5 + 35k^4 + 35k^3 + 21k^2 + 7k}_{\text{div. by } 7}. \blacksquare\end{aligned}$$

2. THE BINOMIAL THEOREM

DEFINITION:
Let n and k be some integers with $0 \leq k \leq n$. Then

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

is called a binomial coefficient.

PROPERTIES:

1. $\binom{n}{0} = \binom{n}{n} = 1.$

Proof: We have

$$\binom{n}{0} = \frac{n!}{0!(n-0)!} = \frac{n!}{1 \cdot n!} = 1,$$

$$\binom{n}{n} = \frac{n!}{n!(n-n)!} = \frac{n!}{n! \cdot 0!} = \frac{n!}{n! \cdot 1} = 1. \blacksquare$$

2. $\binom{n}{1} = \binom{n}{n-1} = n.$

Proof: We have

$$\binom{n}{1} = \frac{n!}{1!(n-1)!} = \frac{(n-1)! \cdot n}{1! \cdot (n-1)!} = n,$$

$$\binom{n}{n-1} = \frac{n!}{(n-1)![n-(n-1)]!} = \frac{n!}{(n-1)! \cdot 1!} = \frac{(n-1)! \cdot n}{(n-1)! \cdot 1!} = n. \blacksquare$$

3. $\binom{n}{k} = \binom{n}{n-k}.$

Proof: We have

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!k!} = \frac{n!}{(n-k)![n-(n-k)]!} = \binom{n}{n-k}. \blacksquare$$

4. $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$.

Proof: We have

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\
&= \frac{n!(n-k+1)}{k!(n-k)!(n-k+1)} + \frac{n!k}{(k-1)!k(n-k+1)!} \\
&= \frac{n!(n-k+1)}{k!(n-k+1)!} + \frac{n!k}{k!(n-k+1)!} \\
&= \frac{n!(n-k+1)+n!k}{k!(n-k+1)!} \\
&= \frac{n!n-n!k+n!+n!k}{k!(n-k+1)!} \\
&= \frac{n!n+n!}{k!(n-k+1)!} \\
&= \frac{n!(n+1)}{k!(n-k+1)!} = \frac{(n+1)!}{k!(n-k+1)!} = \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}. \blacksquare
\end{aligned}$$

PROBLEM:

For all integers n and k with $1 \le k \le n$ we have

$$\binom{n}{k-1} + 2\binom{n}{k} + \binom{n}{k+1} = \binom{n+2}{k+1}.$$

Proof: By property 4 we have

$$\begin{aligned}
\binom{n}{k-1} + 2\binom{n}{k} + \binom{n}{k+1} &= \binom{n}{k-1} + \binom{n}{k} + \binom{n}{k} + \binom{n}{k+1} \\
&= \binom{n+1}{k} + \binom{n+1}{k+1} = \binom{n+2}{k+1}. \blacksquare
\end{aligned}$$

THEOREM (The Binomial Theorem):

Let a and b be any real numbers and let n be any nonnegative integer. Then

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-2}a^2b^{n-2} + \binom{n}{n-1}ab^{n-1} + b^n.$$

PROBLEM:

For all integers $n \geq 1$ we have

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n.$$

Proof: Putting $a = b = 1$ in the Theorem above, we get

$$(1+1)^n$$
$$= 1^n + \binom{n}{1} \cdot 1^{n-1} \cdot 1 + \binom{n}{2} \cdot 1^{n-2} \cdot 1^2 + \ldots + \binom{n}{n-2} \cdot 1^2 \cdot 1^{n-2} + \binom{n}{n-1} \cdot 1 \cdot 1^{n-1} + 1^n,$$

hence

$$2^n = 1 + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-2} + \binom{n}{n-1} + 1,$$

therefore by property 1 we get

$$2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-2} + \binom{n}{n-1} + \binom{n}{n}. \blacksquare$$

PROBLEM:

For all integers $n \geq 1$ we have

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^n \binom{n}{n} = 0.$$

Proof: Putting $a = 1$ and $b = -1$ in the Theorem above, we get

$$(1-1)^n$$
$$= 1^n + \binom{n}{1} \cdot 1^{n-1} \cdot (-1) + \binom{n}{2} \cdot 1^{n-2} \cdot (-1)^2 + \ldots + \binom{n}{n-1} \cdot 1 \cdot (-1)^{n-1} + (-1)^n,$$

hence

$$0 = 1 - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^{n-1} \binom{n}{n-1} + (-1)^n,$$

therefore by property 1 we get

$$0 = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^{n-1} \binom{n}{n-1} + (-1)^n \binom{n}{n}. \blacksquare$$

3. RATIONAL AND IRRATIONAL NUMBERS

DEFINITION:

Rational numbers are all numbers of the form $\dfrac{p}{q}$, where p and q are integers and $q \neq 0$.

EXAMPLE: $\dfrac{1}{2},\ -\dfrac{5}{3},\ 2,\ 0, \dfrac{50}{10}$, etc.

NOTATIONS:

$\mathbb{N}$ = all natural numbers, that is, $1, 2, 3, \ldots$

$\mathbb{Z}$ = all integer numbers, that is, $0, \pm 1, \pm 2, \pm 3, \ldots$

$\mathbb{Q}$ = all rational numbers

$\mathbb{R}$ = all real numbers

DEFINITION:

A number which is not rational is said to be irrational.

PROBLEM 1: Prove that $\sqrt{2}$ is irrational.

Proof: Assume to the contrary that $\sqrt{2}$ is rational, that is

$$\sqrt{2} = \frac{p}{q},$$

where p and q are integers and $q \neq 0$. Moreover, let p and q have no common divisor > 1. Then

$$2 = \frac{p^2}{q^2} \quad \Rightarrow \quad 2q^2 = p^2. \tag{3.1}$$

Since $2q^2$ is even, it follows that p^2 is even. Then p is also even (in fact, if p is odd, then p^2 is odd). This means that there exists $k \in \mathbb{Z}$ such that

$$p = 2k. \tag{3.2}$$

Substituting (3.2) into (3.1), we get

$$2q^2 = (2k)^2 \quad \Rightarrow \quad 2q^2 = 4k^2 \quad \Rightarrow \quad q^2 = 2k^2.$$

Since $2k^2$ is even, it follows that q^2 is even. Then q is also even. This is a contradiction. ■

<u>PROBLEM 2</u>: Prove that $\sqrt[3]{4}$ is irrational.

<u>Proof</u>: Assume to the contrary that $\sqrt[3]{4}$ is rational, that is

$$\sqrt[3]{4} = \frac{p}{q},$$

where p and q are integers and $q \neq 0$. Moreover, let <u>p and q have no common divisor > 1</u>. Then

$$4 = \frac{p^3}{q^3} \quad \Rightarrow \quad 4q^3 = p^3. \tag{3.3}$$

Since $4q^3$ is even, it follows that p^3 is even. Then <u>p is also even</u> (in fact, if p is odd, then p^3 is odd). This means that there exists $k \in \mathbb{Z}$ such that

$$p = 2k. \tag{3.4}$$

Substituting (3.4) into (3.3), we get

$$4q^3 = (2k)^3 \quad \Rightarrow \quad 4q^3 = 8k^3 \quad \Rightarrow \quad q^3 = 2k^3.$$

Since $2k^3$ is even, it follows that q^3 is even. Then <u>q is also even</u>. This is a contradiction. ■

<u>PROBLEM 3</u>: Prove that $\sqrt{6}$ is irrational.

<u>Proof</u>: Assume to the contrary that $\sqrt{6}$ is rational, that is

$$\sqrt{6} = \frac{p}{q},$$

where p and q are integers and $q \neq 0$. Moreover, let <u>p and q have no common divisor > 1</u>. Then

$$6 = \frac{p^2}{q^2} \quad \Rightarrow \quad 6q^2 = p^2. \tag{3.5}$$

Since $6q^2$ is even, it follows that p^2 is even. Then <u>p is also even</u> (in fact, if p is odd, then p^2 is odd). This means that there exists $k \in \mathbb{Z}$ such that

$$p = 2k. \tag{3.6}$$

Substituting (3.6) into (3.5), we get

$$6q^2 = (2k)^2 \quad \Rightarrow \quad 6q^2 = 4k^2 \quad \Rightarrow \quad 3q^2 = 2k^2.$$

Since $2k^2$ is even, it follows that $3q^2$ is even. Then <u>q is also even</u> (in fact, if q is odd, then $3q^2$ is odd). This is a contradiction. ■

PROBLEM 4: Prove that $\frac{1}{3}\sqrt{2}+5$ is irrational.

Proof: Assume to the contrary that $\frac{1}{3}\sqrt{2}+5$ is rational, that is

$$\frac{1}{3}\sqrt{2}+5=\frac{p}{q},$$

where p and q are integers and $q \neq 0$. Then

$$\sqrt{2}=\frac{3(p-5q)}{q}.$$

Since $\sqrt{2}$ is irrational and $\frac{3(p-5q)}{q}$ is rational, we obtain a contradiction. ■

PROBLEM 5: Prove that $\log_5 2$ is irrational.

Proof: Assume to the contrary that $\log_5 2$ is rational, that is

$$\log_5 2=\frac{p}{q},$$

where p and q are integers and $q \neq 0$. Then

$$5^{p/q}=2 \quad \Rightarrow \quad 5^p=2^q.$$

Since 5^p is odd and 2^q is even, we obtain a contradiction. ■

4. DIVISION ALGORITHM

<u>PROBLEM</u>: Prove that $\sqrt{3}$ is irrational.

<u>Proof</u>: Assume to the contrary that $\sqrt{3}$ is rational, that is

$$\sqrt{3} = \frac{p}{q},$$

where p and q are integers and $q \neq 0$. Moreover, let <u>p and q have no common divisor > 1</u>. Then

$$3 = \frac{p^2}{q^2} \quad \Rightarrow \quad 3q^2 = p^2.$$

Since $3q^2$ is divisible by 3, it follows that p^2 is divisible by 3. Then <u>p is also divisible by 3</u> (in fact, if p is not divisible by 3, then ...???

<u>THEOREM</u> (DIVISION ALGORITHM): *For any integers a and b with $a \neq 0$ there exist unique integers q and r such that*

$$b = aq + r, \quad \textit{where} \quad 0 \leq r < |a|.$$

The integers q and r are called the **quotient** *and the* **reminder** *respectively.*

<u>EXAMPLE 1</u>: Let $b = 49$ and $a = 4$, then $49 = 4 \cdot 12 + 1$, so the quotient is 12 and the reminder is 1.

<u>REMARK</u>: We can also write 49 as $3 \cdot 12 + 13$, but in this case 13 is not a reminder, since it is NOT less than 3.

<u>EXAMPLE 2</u>: Let $a = 2$. Since $0 \leq r < 2$, then for any integer number b we have ONLY TWO possibilities:

$$b = 2q \quad \text{or} \quad b = 2q + 1.$$

So, thanks to the Division Algorithm we <u>proved</u> that any integer number is either even or odd.

<u>EXAMPLE 3</u>: Let $a = 3$. Since $0 \leq r < 3$, then for any integer number b we have ONLY THREE possibilities:

$$b = 3q, \quad b = 3q + 1, \quad \text{or} \quad b = 3q + 2.$$

<u>Proof of the Problem</u>: Assume to the contrary that $\sqrt{3}$ is rational, that is

$$\sqrt{3} = \frac{a}{b},$$

where a and b are integers and $b \neq 0$. Moreover, let <u>a and b have no common divisor > 1</u>. Then

$$3 = \frac{a^2}{b^2} \quad \Rightarrow \quad 3b^2 = a^2. \tag{4.1}$$

Since $3b^2$ is divisible by 3, it follows that a^2 is divisible by 3. Then $\underline{a \text{ is also divisible by } 3.}$

In fact, if a is not divisible by 3, then by the Division Algorithm there exists $q \in \mathbb{Z}$ such that

$$a = 3q + 1 \quad \text{or} \quad a = 3q + 2.$$

Suppose $a = 3q + 1$, then

$$a^2 = (3q+1)^2 = 9q^2 + 6q + 1 = 3(\underbrace{3q^2 + 2q}_{q'}) + 1 = 3q' + 1,$$

which is not divisible by 3. We get a contradiction. Similarly, if $a = 3q + 2$, then

$$a^2 = (3q+2)^2 = 9q^2 + 12q + 4 = 3(\underbrace{3q^2 + 4q + 1}_{q''}) + 1 = 3q'' + 1,$$

which is not divisible by 3. We get a contradiction again.

So, we proved that if a^2 is divisible by 3, then $\underline{a \text{ is also divisible by } 3.}$ This means that there exists $q \in \mathbb{Z}$ such that

$$a = 3q. \tag{4.2}$$

Substituting (4.2) into (4.1), we get

$$3b^2 = (3q)^2 \quad \Rightarrow \quad 3b^2 = 9q^2 \quad \Rightarrow \quad b^2 = 3q^2.$$

Since $3q^2$ is divisible by 3, it follows that b^2 is divisible by 3. Then $\underline{b \text{ is also divisible by } 3}$ by the arguments above. This is a contradiction. ■

5. GREATEST COMMON DIVISOR AND EUCLID'S LEMMA

PROBLEM: Prove that $\sqrt{101}$ is irrational.

Proof: Assume to the contrary that $\sqrt{101}$ is rational, that is

$$\sqrt{101} = \frac{a}{b},$$

where a and b are integers and $b \neq 0$. Moreover, let a and b have no common divisor > 1. Then

$$101 = \frac{a^2}{b^2} \quad \Rightarrow \quad 101b^2 = a^2.$$

Since $101b^2$ is divisible by 101, it follows that a^2 is divisible by 101. Then a is also divisible by 101.
In fact, if a is not divisible by 101, then by the Division Algorithm there exists $q \in \mathbb{Z}$ such that

$$a = 101q + 1 \quad \text{or} \quad a = 101q + 2 \quad \text{or} \quad a = 101q + 3 \quad \text{or} \quad a = 101q + 4 \ldots ???$$

DEFINITION:

If a and b are integers with $a \neq 0$, we say that a is a divisor of b if there exists an integer q such that $b = aq$. We also say that a divides b and we denote this by

$$a \mid b.$$

EXAMPLE: We have: $4 \mid 12$, since $12 = 4 \cdot 3$
$4 \nmid 15$, since $15 = 4 \cdot 3.75$

DEFINITION:

A common divisor of nonzero integers a and b is an integer c such that $c \mid a$ and $c \mid b$. The greatest common divisor (gcd) of a and b, denoted by (a, b), is the largest common divisor of integers a and b.

EXAMPLE: The common divisors of 24 and 84 are $\pm 1, \ \pm 2, \ \pm 3, \ \pm 4, \ \pm 6$, and ± 12. Hence, $(24, 84) = 12$. Similarly, looking at sets of common divisors, we find that $(15, 81) = 3, \ (100, 5) = 5, \ (17, 25) = 1, (-17, 289) = 17$, etc.

THEOREM: If a and b are nonzero integers, then their gcd is a linear combination of a and b, that is there exist integer numbers s and t such that

$$sa + tb = (a, b).$$

Proof: Let d be the least positive integer that is a linear combination of a and b. We write

$$d = sa + tb, \tag{5.1}$$

where s and t are integers.

We first show that $d \mid a$. By the Division Algorithm we have

$$a = dq + r, \text{ where } 0 \leq r < d.$$

From this and (5.1) it follows that

$$r = a - dq = a - q(sa + tb) = a - qsa - qtb = (1 - qs)a + (-qt)b.$$

This shows that r is a linear combination of a and b. Since $0 \leq r < d$, and d is the least positive linear combination of a and b, we conclude that $r = 0$, and hence $d \mid a$. In a similar manner, we can show that $d \mid b$.

We have shown that d is a common divisor of a and b. We now show that d is the *greatest common divisor* of a and b. Assume to the contrary that

$$(a, b) = d' \quad \text{and} \quad d' > d.$$

Since $d' \mid a$, $d' \mid b$, and $d = sa + tb$, it follows that $d' \mid d$, therefore $d' \leq d$. We obtain a contradiction. So, d is the greatest common divisor of a and b and this concludes the proof. ■

DEFINITION:

An integer $n \geq 2$ is called prime if its only positive divisors are 1 and n. Otherwise, n is called composite.

EXAMPLE: Numbers $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59 \ldots$ are prime.

THEOREM (Euclid's Lemma): If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$. More generally, if a prime p divides a product $a_1 a_2 \ldots a_n$, then it must divide at least one of the factors a_i.

Proof: Assume that $p \nmid a$. We must show that $p \mid b$. By the theorem above, there are integers s and t with

$$sp + ta = (p, a).$$

Since p is prime and $p \nmid a$, we have $(p, a) = 1$, and so

$$sp + ta = 1.$$

Multiplying both sides by b, we get

$$spb + tab = b. \tag{5.2}$$

Since $p \mid ab$ and $p \mid spb$, it follows that

$$p \mid (spb + tab).$$

This and (5.2) give $p \mid b$. This completes the proof of the first part of the theorem. The second part (generalization) easily follows by induction on $n \geq 2$. ■

COROLLARY: If p is a prime and $p \mid a^2$, then $p \mid a$.

Proof: Put $a = b$ in Euclid's Lemma. ■

<u>THEOREM</u>: Let p be a prime. Then $\sqrt{p}$ is irrational.

<u>Proof</u>: Assume to the contrary that $\sqrt{p}$ is rational, that is

$$\sqrt{p} = \frac{a}{b},$$

where a and b are integers and $b \neq 0$. Moreover, let <u>a and b have no common divisor > 1</u>. Then

$$p = \frac{a^2}{b^2} \quad \Rightarrow \quad pb^2 = a^2. \tag{5.3}$$

Since pb^2 is divisible by p, it follows that a^2 is divisible by p. Then <u>a is also divisible by p</u> by the Corollary above. This means that there exists $q \in \mathbb{Z}$ such that

$$a = pq. \tag{5.4}$$

Substituting (5.4) into (5.3), we get

$$pb^2 = (pq)^2 \;\; \Rightarrow \;\; b^2 = pq^2.$$

Since pq^2 is divisible by p, it follows that b^2 is divisible by p. Then <u>b is also divisible by p</u> by the Corollary above. This is a contradiction. ■

<u>PROBLEM</u>: Prove that $\sqrt{101}$ is irrational.

<u>Proof</u>: Since 101 is prime, the result immediately follows from the Theorem above. ■

<u>PROBLEM</u>: Prove that if a and b are positive integers with $(a, b) = 1$, then $(a^2, b^2) = 1$ for all $n \in \mathbb{Z}^+$.

<u>Proof 1</u>: Assume to the contrary that $(a^2, b^2) = n > 1$. Then there is a prime p such that $p \mid a^2$ and $p \mid b^2$. From this by Euclid's Lemma it follows that $p \mid a$ and $p \mid b$, therefore $(a, b) \geq p$. This is a contradiction. ■

<u>Proof 2</u> (Hint): Use the Fundamental Theorem of Arithmetic below.

6. FUNDAMENTAL THEOREM OF ARITHMETIC

THEOREM (Fundamental Theorem of Arithmetic): Assume that an integer $a \geq 2$ has factorizations

$$a = p_1 \dots p_m \quad \text{and} \quad a = q_1 \dots q_n,$$

where the p's and q's are primes. Then $n = m$ and the $q's$ may be reindexed so that $q_i = p_i$ for all i.

Proof: We prove by induction on ℓ, the larger of m and n, i. e. $\ell = \max(m, n)$.

Step 1. If $\ell = 1$, then the given equation in $a = p_1 = q_1$, and the result is obvious.

Step 2. Suppose the theorem holds for some $\ell = k \geq 1$.

Step 3. We prove it for $\ell = k + 1$. Let

$$a = p_1 \dots p_m = q_1 \dots q_n, \tag{6.1}$$

where

$$\max(m, n) = k + 1. \tag{6.2}$$

From (6.1) it follows that $p_m \mid q_1 \dots q_n$, therefore by Euclid's Lemma there is some q_i such that $p_m \mid q_i$. But q_i, being a prime, has no positive divisors other than 1, therefore $p_m = q_i$. Reindexing, we may assume that $q_n = p_m$. Canceling, we have

$$p_1 \dots p_{m-1} = q_1 \dots q_{n-1}.$$

Moreover, $\max(m - 1, n - 1) = k$ by (6.2). Therefore by step 2 q's may be reindexed so that $q_i = p_i$ for all i; plus, $m - 1 = n - 1$, hence $m = n$. ■

COROLLARY: If $a \geq 2$ is an integer, then there are unique distinct primes p_i and unique integers $e_i > 0$ such that

$$a = p_1^{e_1} \dots p_n^{e_n}.$$

Proof: Just collect like terms in a prime factorization. ■

EXAMPLE: $120 = 2^3 \cdot 3 \cdot 5$.

PROBLEM: Prove that $\log_3 5$ is irrational.

Proof: Assume to the contrary that $\log_3 5$ is rational, that is

$$\log_3 5 = \frac{p}{q},$$

where p and q are integers and $q \neq 0$. Then

$$3^{p/q} = 5 \quad \Rightarrow \quad 3^p = 5^q,$$

which contradicts the Fundamental Theorem of Arithmetic. ■

7. EUCLIDEAN ALGORITHM

<u>THEOREM</u> (Euclidean Algorithm): Let a and b be positive integers. Then there is an algorithm that finds (a,b).

<u>LEMMA</u>: If a,b,q,r are integers and $a=bq+r$, then $(a,b)=(b,r)$.

<u>Proof</u>: We have $(a,b)=(bq+r,b)=(b,r)$. ■

<u>Proof of the Theorem</u>: The idea is to keep repeating the division algorithm. We have:

$$\begin{aligned}
a &= bq_1+r_1, \quad (a,b)=(b,r_1)\\
b &= r_1q_2+r_2, \quad (b,r_1)=(r_1,r_2)\\
r_1 &= r_2q_3+r_3, \quad (r_1,r_2)=(r_2,r_3)\\
r_2 &= r_3q_4+r_4, \quad (r_2,r_3)=(r_3,r_4)\\
&\ldots\\
r_{n-2} &= r_{n-1}q_n+r_n, \quad (r_{n-2},r_{n-1})=(r_{n-1},r_n)\\
r_{n-1} &= r_nq_{n+1}, \quad (r_{n-1},r_n)=r_n,
\end{aligned}$$

therefore

$$(a,b)=(b,r_1)=(r_1,r_2)=(r_2,r_3)=(r_3,r_4)=\ldots=(r_{n-2},r_{n-1})=(r_{n-1},r_n)=r_n.$$

■

<u>PROBLEM</u>: Find $(326,78)$.

<u>Solution</u>: By the Euclidean Algorithm we have

$$\begin{aligned}
326 &= 78\cdot 4+14\\
78 &= 14\cdot 5+8\\
14 &= 8\cdot 1+6\\
8 &= 6\cdot 1+2\\
6 &= 2\cdot 3
\end{aligned}$$

therefore $(326,78)=2$.

<u>PROBLEM</u>: Find $(252,198)$.

<u>Solution</u>: By the Euclidean Algorithm we have

$$\begin{aligned}
252 &= 198\cdot 1+54\\
198 &= 54\cdot 3+36\\
54 &= 36\cdot 1+18\\
36 &= 18\cdot 2
\end{aligned}$$

therefore $(252,198)=18$.

PROBLEM: Find $(4361, 42371)$.

Solution: By the Euclidean Algorithm we have

$$\begin{aligned} 42371 &= 9 \cdot 4361 + 3122 \\ 4361 &= 1 \cdot 3122 + 1239 \\ 3122 &= 2 \cdot 1239 + 644 \\ 1239 &= 1 \cdot 644 + 595 \\ 644 &= 1 \cdot 595 + 49 \\ 595 &= 12 \cdot 49 + 7 \\ 49 &= 7 \cdot 7 + 0, \end{aligned}$$

therefore $(4361, 42371) = 7$.

THEOREM: Let $a = p_1^{e_1} \ldots p_n^{e_n}$ and $b = p_1^{f_1} \ldots p_n^{f_n}$ be positive integers. Then

$$(a, b) = p_1^{\min(e_1, f_1)} \ldots p_n^{\min(e_n, f_n)}.$$

EXAMPLE: Since $720 = 2^4 \cdot 3^2 \cdot 5$ and $2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$, we have:

$$(720, 2100) = 2^2 \cdot 3 \cdot 5 = 60.$$

PROBLEM: Let $a \in \mathbb{Z}$. Prove that $(2a + 3, a + 2) = 1$.

Proof: By the Lemma above we have

$$\begin{aligned} (2a + 3, a + 2) &= (a + 1 + a + 2, a + 2) \\ &= (a + 1, a + 2) \\ &= (a + 1, a + 1 + 1) \\ &= (a + 1, 1) \\ &= 1. \blacksquare \end{aligned}$$

PROBLEM: Let $a \in \mathbb{Z}$. Prove that $(7a + 2, 10a + 3) = 1$.

Proof: By the Lemma above we have

$$\begin{aligned} (7k + 2,\ 10k + 3) &= (7k + 2,\ 7k + 2 + 3k + 1) \\ &= (7k + 2,\ 3k + 1) \\ &= (6k + 2 + k,\ 3k + 1) \\ &= (k,\ 3k + 1) \\ &= (k,\ 1) \\ &= 1. \blacksquare \end{aligned}$$

8. FERMAT'S LITTLE THEOREM

<u>Theorem (Fermat's Little Theorem)</u>: Let p be a prime. We have

$$p \mid n^p - n \tag{8.1}$$

for any integer $n \geq 1$.

<u>Proof 1</u>:

STEP 1: For n=1 (8.1) is true, since

$$p \mid 1^p - 1.$$

STEP 2: Suppose (8.1) is true for some $n = k \geq 1$, that is

$$p \mid k^p - k.$$

STEP 3: Prove that (8.1) is true for $n = k + 1$, that is

$$p \mid (k+1)^p - (k+1).$$

<u>Lemma:</u> Let p be a prime and ℓ be an integer with $1 \leq \ell \leq p - 1$. Then

$$p \mid \binom{p}{\ell}.$$

<u>Proof</u>: We have

$$\binom{p}{\ell} = \frac{p!}{\ell!(p-\ell)!} = \frac{\ell!(\ell+1)\cdot\ldots\cdot p}{\ell!(p-\ell)!} = \frac{(\ell+1)\cdot\ldots\cdot p}{(p-\ell)!},$$

therefore

$$\binom{p}{\ell}(p-\ell)! = (\ell+1)\cdot\ldots\cdot p.$$

Form this it follows that

$$p \mid \binom{p}{\ell}(p-\ell)!,$$

hence by Euclid's Lemma p divides $\binom{p}{\ell}$ or $(p-\ell)!$. It is easy to see that $p \not\mid (p-\ell)!$. Therefore $p \mid \binom{p}{\ell}$.

We have

$$\begin{aligned}
&(k+1)^p - (k+1) \\
&= k^p + \binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + \ldots + \binom{p}{p-1}k + 1 - k - 1 \\
&= \underbrace{k^p - k}_{\substack{\text{St. 2} \\ \text{div. by p}}} + \underbrace{\binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + \ldots + \binom{p}{p-1}k}_{\text{div. by p by Lemma}}. \blacksquare
\end{aligned}$$

9. CONGRUENCES

DEFINITION:

Let m be a positive integer. Then integers a and b are congruent modulo m, denoted by

$$a \equiv b \bmod m,$$

if $m \mid (a - b)$.

EXAMPLE:

$$3 \equiv 1 \bmod 2, \quad 6 \equiv 4 \bmod 2, \quad -14 \equiv 0 \bmod 7, \quad 25 \equiv 16 \bmod 9, \quad 43 \equiv -27 \bmod 35.$$

PROPERTIES:

Let m be a positive integer and let a, b, c, d be integers. Then

1. $a \equiv a \bmod m$
2. If $a \equiv b \bmod m$, then $b \equiv a \bmod m$.
3. If $a \equiv b \bmod m$ and $b \equiv c \bmod m$, then $a \equiv c \bmod m$.
4. (a) If $a \equiv qm + r \bmod m$, then $a \equiv r \bmod m$.

   (b) Every integer a is congruent mod m to exactly one of $0, 1, \ldots, m - 1$.
5. If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then

$$a \pm c \equiv b \pm d \bmod m \quad \text{and} \quad ac \equiv bd \bmod m.$$

$5'$. If $a \equiv b \bmod m$, then

$$a \pm c \equiv b \pm c \bmod m \quad \text{and} \quad ac \equiv bc \bmod m.$$

$5''$. If $a \equiv b \bmod m$, then

$$a^n \equiv b^n \bmod m \quad \text{for any } n \in \mathbb{Z}^+.$$

6. If $(c, m) = 1$ and $ac \equiv bc \bmod m$, then $a \equiv b \bmod m$.

Proof 2 of Fermat's Little Theorem: We distinguish two cases.

Case A: Let $p \mid n$, then, obviously, $p \mid n^p - n$, and we are done.

Case B: Let $p \nmid n$. Since p is prime, we have

$$(p, n) = 1. \tag{9.1}$$

Consider the following numbers:

$$n,\ 2n,\ 3n, \ldots, (p - 1)n.$$

We have

$$\begin{aligned} &n \equiv r_1 \bmod p \\ &2n \equiv r_2 \bmod p \\ &3n \equiv r_3 \bmod p \\ &\dots \\ &(p-1)n \equiv r_{p-1} \bmod p, \end{aligned} \tag{9.2}$$

where $0 \le r_i \le p-1$. Moreover, $r_i \ne 0$, since otherwise $p \mid in$, and therefore by Euclid'd Lemma $p \mid i$ or $p \mid n$. But this is impossible, since $p > i$ and $p \not\mid n$. So,

$$1 \le r_i \le p-1. \tag{9.3}$$

From (9.2) by property 5 we have

$$n \cdot 2n \cdot 3n \dots (p-1)n \equiv r_1 r_2 \dots r_{p-1} \bmod p$$

$$\Downarrow$$

$$(p-1)! n^{p-1} \equiv r_1 r_2 \dots r_{p-1} \bmod p. \tag{9.4}$$

<u>Lemma:</u> We have

$$r_1 r_2 \dots r_{p-1} = (p-1)!. \tag{9.5}$$

<u>Proof</u>: We first show that

$$r_1, r_2, \dots, r_{p-1} \quad \text{are all distinct.} \tag{9.6}$$

In fact, assume to the contrary that there are some r_i and r_j with $r_i = r_j$. Then by (9.2) we have $in \equiv jn \bmod p$, therefore by property 6 with (9.1) we get $i \equiv j \bmod p$, which is impossible. This contradiction proves (9.6).

By the Lemma we have

$$r_1 r_2 \dots r_{p-1} = (p-1)!. \tag{9.7}$$

By (9.4) and (9.7) we obtain

$$(p-1)! n^{p-1} \equiv (p-1)! \bmod p.$$

Since $(p, (p-1)!) = 1$, from this by by property 6 we get

$$n^{p-1} \equiv 1 \bmod p,$$

hence

$$n^p \equiv n \bmod p$$

by property $4'$. This means that $n^p - n$ is divisible by p. ■

<u>COROLLARY</u>: Let p be a prime. Then

$$n^{p-1} \equiv 1 \bmod p$$

for any integer $n \ge 1$ with $(n, p) = 1$.

<u>THEOREM</u>: If $(a, m) = 1$, then, for every integer b, the congruence

$$ax \equiv b \bmod m \tag{9.8}$$

has exactly one solution

$$x \equiv bs \mod m, \tag{9.9}$$

where s is such number that

$$as \equiv 1 \mod m. \tag{9.10}$$

Proof (Sketch): We show that (9.9) is the solution of (9.8). In fact, if we multiply (9.9) by a and (9.10) by b (we can do that by property $5'$), we get

$$ax \equiv abs \mod m \quad \text{and} \quad bsa \equiv b \mod m,$$

which imply (9.8) by property 3. ■

Problems

Problem 1: Find all solutions of the congruence

$$2x \equiv 1 \mod 3.$$

Solution: We first note that $(2, 3) = 1$. Therefore we can apply the theorem above. Since $2 \cdot 2 \equiv 1 \mod 3$, we get

$$x \equiv 1 \cdot 2 \equiv 2 \mod 3.$$

Problem 2: Find all solutions of the following congruence

$$2x \equiv 5 \mod 7.$$

Solution: We first note that $(2, 7) = 1$. Therefore we can apply the theorem above. Since $2 \cdot 4 \equiv 1 \mod 7$, we get

$$x \equiv 5 \cdot 4 \equiv 6 \mod 7.$$

Problem 3: Find all solutions of the congruence

$$3x \equiv 4 \mod 8.$$

Solution: We first note that $(3, 8) = 1$. Therefore we can apply the theorem above. Since $3 \cdot 3 \equiv 1 \mod 8$, we get

$$x \equiv 4 \cdot 3 \equiv 12 \equiv 4 \mod 8.$$

Problem 4: Find all solutions of the following congruence

$$2x \equiv 5 \mod 8.$$

<u>Solution</u>: Since $(2, 8) = 2$, we can't apply the theorem above directly. We now note that $2x \equiv 5 \bmod 8$ is equivalent to $2x - 8y = 5$, which is impossible, since the left-hand side is divisible by 2, whereas the right-hand side is not. So, this equation has no solutions.

<u>Problem 5</u>: Find all solutions of the congruence

$$8x \equiv 7 \bmod 18.$$

<u>Solution</u>: Since $(8, 18) = 2$, we can't apply the theorem above directly. We now note that $8x \equiv 7 \bmod 18$ is equivalent to $8x - 18y = 7$, which is impossible, since the left-hand side is divisible by 2, whereas the right-hand side is not. So, this equation has no solutions.

<u>Problem 6</u>: Find all solutions of the following congruence

$$4x \equiv 2 \bmod 6.$$

<u>Solution</u>: Since $(4, 6) = 2$, we can't apply the theorem above directly again. However, canceling out 2 (think about that!), we obtain

$$2x \equiv 1 \bmod 3.$$

Note that $(2, 3) = 1$. Therefore we can apply the theorem above to the new equation. Since $2 \cdot 2 \equiv 1 \bmod 3$, we get

$$x \equiv 1 \cdot 2 \equiv 2 \bmod 3.$$

<u>Problem 7</u>: Find all solutions of the congruence

$$6x \equiv 3 \bmod 15.$$

<u>Solution</u>: Since $(6, 15) = 3$, we can't apply the theorem above directly again. However, canceling out 3, we obtain

$$2x \equiv 1 \bmod 5.$$

Note that $(2, 5) = 1$. Therefore we can apply the theorem above to the new equation. Since $2 \cdot 3 \equiv 1 \bmod 5$, we get

$$x \equiv 1 \cdot 3 \equiv 3 \bmod 5.$$

<u>Problem 8</u>: Find all solutions of the congruence

$$9x + 23 \equiv 28 \bmod 25.$$

Solution: We first rewrite this congruence as

$$9x \equiv 5 \bmod 25.$$

Note that $(9, 25) = 1$. Therefore we can apply the theorem above. Since $9 \cdot 14 \equiv 1 \bmod 25$, we get

$$x \equiv 5 \cdot 14 \equiv 70 \equiv 20 \bmod 25.$$

Problem 9: What is the last digit of 345271^{79399}?

Solution: It is obvious that

$$345271 \equiv 1 \bmod 10,$$

therefore by property $5''$ we have

$$345271^{79399} \equiv 1^{79399} \equiv 1 \bmod 10.$$

This means that the last digit of 345271^{79399} is 1.

Problem 10: What is the last digit of 4321^{4321}?

Solution: It is obvious that

$$4321 \equiv 1 \bmod 10,$$

therefore by property $5''$ we have

$$4321^{4321} \equiv 1^{4321} \equiv 1 \bmod 10.$$

This means that the last digit is 1.

Problem 11: Prove that there is no perfect square a^2 which is congruent to 2 or 3 mod 4.

Solution 1: By the property 4(b) each integer number is congruent to 0 or 1 mod 2. Consider all these cases and use property 4(a):

If $a \equiv 0 \bmod 2$, then $a = 2k$, therefore $a^2 = 4k^2$, hence $a^2 \equiv 0 \bmod 4$.

If $a \equiv 1 \bmod 2$, then $a = 2k + 1$, therefore $a^2 = 4k^2 + 4k + 1$, hence $a^2 \equiv 1 \bmod 4$.

So, $a^2 \equiv 0$ or $1 \bmod 4$. Therefore $a^2 \not\equiv 2$ or $3 \bmod 4$.

Solution 2: By the property 4(b) each integer number is congruent to $0, 1, 2$, or $3 \bmod 4$. Consider all these cases and use property $5''$:

If $a \equiv 0 \bmod 4$, then $a^2 \equiv 0^2 \equiv 0 \bmod 4$.

If $a \equiv 1 \bmod 4$, then $a^2 \equiv 1^2 \equiv 1 \bmod 4$.

If $a \equiv 2 \bmod 4$, then $a^2 \equiv 2^2 \equiv 0 \bmod 4$.

If $a \equiv 3 \bmod 4$, then $a^2 \equiv 3^2 \equiv 1 \bmod 4$.

So, $a^2 \equiv 0$ or $1 \bmod 4$. Therefore $a^2 \not\equiv 2$ or $3 \bmod 4$.

<u>Problem 12</u>: Prove that there is no integers a such that a^4 is congruent to 2 or 3 mod 4.

<u>Solution</u>: By the property 4(b) each integer number is congruent to $0, 1, 2$, or 3 mod 4. Consider all these cases and use property $5''$:

If $a \equiv 0 \bmod 4$, then $a^4 \equiv 0^4 \equiv 0 \bmod 4$.
If $a \equiv 1 \bmod 4$, then $a^4 \equiv 1^4 \equiv 1 \bmod 4$.
If $a \equiv 2 \bmod 4$, then $a^4 \equiv 2^4 \equiv 0 \bmod 4$.
If $a \equiv 3 \bmod 4$, then $a^4 \equiv 3^4 \equiv 1 \bmod 4$.

So, $a^4 \equiv 0$ or $1 \bmod 4$. Therefore $a^4 \not\equiv 2$ or $3 \bmod 4$.

<u>Problem 13</u>: Prove that there is no perfect square a^2 whose last digit is $2, 3, 7$ or 8.

<u>Solution</u>: By the property 4(b) each integer number is congruent to $0, 1, 2, \ldots, 8$ or 9 mod 10. Consider all these cases and use property $5''$:

If $a \equiv 0 \bmod 10$, then $a^2 \equiv 0^2 \equiv 0 \bmod 10$.
If $a \equiv 1 \bmod 10$, then $a^2 \equiv 1^2 \equiv 1 \bmod 10$.
If $a \equiv 2 \bmod 10$, then $a^2 \equiv 2^2 \equiv 4 \bmod 10$.
If $a \equiv 3 \bmod 10$, then $a^2 \equiv 3^2 \equiv 9 \bmod 10$.
If $a \equiv 4 \bmod 10$, then $a^2 \equiv 4^2 \equiv 6 \bmod 10$.
If $a \equiv 5 \bmod 10$, then $a^2 \equiv 5^2 \equiv 5 \bmod 10$.
If $a \equiv 6 \bmod 10$, then $a^2 \equiv 6^2 \equiv 6 \bmod 10$.
If $a \equiv 7 \bmod 10$, then $a^2 \equiv 7^2 \equiv 9 \bmod 10$.
If $a \equiv 8 \bmod 10$, then $a^2 \equiv 8^2 \equiv 4 \bmod 10$.
If $a \equiv 9 \bmod 10$, then $a^2 \equiv 9^2 \equiv 1 \bmod 10$.

So, $a^2 \equiv 0, 1, 4, 5, 6$ or $9 \bmod 10$. Therefore $a^2 \not\equiv 2, 3, 7$ or $8 \bmod 10$, and the result follows.

<u>Problem 14</u>: Prove that 44444444444444444443 is not a perfect square.

<u>Solution</u>: The last digit is 3, which is impossible by Problem 13.

<u>Problem 15</u>: Prove that $888\ldots882$ is not a perfect square.

<u>Solution 1</u>: The last digit is 2, which is impossible by Problem 13.

<u>Solution 2</u>: We have $888\ldots882 = 4k+2$. Therefore it is congruent to 2 mod 4 by property 4(a), which is impossible by Problem 11.

<u>Problem 16</u>: Prove that there is no perfect square a^2 whose last digits are 85.

<u>Solution</u>: It follows from problem 13 that $a^2 \equiv 5 \bmod 10$ only if $a \equiv 5 \bmod 10$. Therefore $a^2 \equiv 85 \bmod 100$ only if $a \equiv 5, 15, 25, \ldots, 95 \bmod 100$. If we consider all these cases and use property $5''$ is the same manner as in problem 13, we will see that $a^2 \equiv 25 \bmod 100$. Therefore $a^2 \not\equiv 85 \bmod 100$, and the result follows.

Problem 17: Prove that the equation

$$x^4 - 4y = 3$$

has no solutions in integer numbers.

Solution: Rewrite this equation as

$$x^4 = 4y + 3,$$

which means that

$$x^4 \equiv 3 \bmod 4,$$

which is impossible by Problem 12.

Problem 18: Prove that the equation

$$x^2 - 3y = 5$$

has no solutions in integer numbers.

Solution: Rewrite this equation as

$$x^2 = 3y + 5,$$

which means that

$$x^2 \equiv 5 \equiv 2 \bmod 3.$$

By the property 4(a) each integer number is congruent to $0, 1$, or 2 mod 3. Consider all these cases and use property $5''$:

If $a \equiv 0 \bmod 3$, then $a^2 \equiv 0^2 \equiv 0 \bmod 3$.
If $a \equiv 1 \bmod 3$, then $a^2 \equiv 1^2 \equiv 1 \bmod 3$.
If $a \equiv 2 \bmod 4$, then $a^2 \equiv 2^2 \equiv 1 \bmod 3$.
So, $a^2 \equiv 0$ or $1 \bmod 3$. Therefore $a^2 \not\equiv 2 \bmod 3$.

Problem 19: Prove that the equation

$$3x^2 - 4y = 5$$

has no solutions in integer numbers.

Solution: Rewrite this equation as

$$3x^2 = 4y + 5,$$

which means that

$$3x^2 \equiv 5 \equiv 1 \bmod 4.$$

On the other hand, by Problem 11 we have $x^2 \equiv 0$ or $1 \bmod 4$, hence $3x^2 \equiv 0$ or $3 \bmod 4$. Therefore $x^2 \not\equiv 1 \bmod 4$.

Problem 20: Prove that the equation

$$x^2 - y^2 = 2002$$

has no solutions in integer numbers.

Solution: By Problem 11 we have $x^2 \equiv 0$ or 1 mod 4, hence $x^2 - y^2 \equiv 0, 1$ or -1 mod 4. On the other hand, $2002 \equiv 2$ mod 4. Therefore $x^2 - y^2 \not\equiv 2002$ mod 4,

Problem 21: Prove that $10 \mid 11^{10} - 1$.

Solution: We have $11 \equiv 1$ mod 10, therefore by property $5''$ we get $11^{10} \equiv 1^{10} \equiv 1$ mod 10, which means that $10 \mid 11^{10} - 1$.

Problem 22: Prove that $10 \mid 101^{2003} - 1$.

Solution: We have

$$101 \equiv 1 \bmod 10,$$

therefore by property $5''$ we get

$$101^{2003} \equiv 1^{2003} \equiv 1 \bmod 10,$$

which means that $10 \mid 101^{2003} - 1$.

Problem 23: Prove that $23 \mid a^{154} - 1$ for any $a \in \mathbb{Z}^+$ with $(a, 23) = 1$.

Solution: By Fermat's Little theorem we have

$$a^{22} \equiv 1 \bmod 23,$$

therefore by property $5''$ we get

$$a^{22 \cdot 7} \equiv 1^7 \equiv 1 \bmod 23,$$

and the result follows.

Problem 24: Prove that $17 \mid a^{80} - 1$ for any $a \in \mathbb{Z}^+$ with $(a, 17) = 1$.

Solution: By Fermat's Little theorem we have $a^{16} \equiv 1$ mod 17, therefore by property $5''$ we get $a^{16 \cdot 5} \equiv 1^5 \equiv 1$ mod 17, and the result follows.

Problem 25: What is the remainder after dividing 3^{50} by 7?

Solution: By Fermat's Little theorem we have $3^6 \equiv 1$ mod 7, therefore by property $5''$ we get $3^{6 \cdot 8} \equiv 1^{48} \equiv 1$ mod 7, therefore $3^{50} \equiv 9 \equiv 2$ mod 7.

10. PERMUTATIONS

DEFINITION:
A permutation of a set X is a rearrangement of its elements.

EXAMPLE:

1. Let $X = \{1, 2\}$. Then there are 2 permutations:

$$12, \ 21.$$

2. Let $X = \{1, 2, 3\}$. Then there are 6 permutations:

$$123, \ 132, \ 213, \ 231, \ 312, \ 321.$$

3. Let $X = \{1, 2, 3, 4\}$. Then there are 24 permutations:

$$\begin{array}{cccccc} 1234, & 1243, & 1324, & 1342, & 1423, & 1432 \\ 2134, & 2143, & 2314, & 2341, & 2413, & 2431 \\ 3214, & 3241, & 3124, & 3142, & 3421, & 3412 \\ 4231, & 4213, & 4321, & 4312, & 4123, & 4132 \end{array}$$

REMARK:
One can show that there are exactly $n!$ permutations of the n-element set X.

DEFINITION′:
A permutation of a set X is a one-one correspondence (a bijection) from X to itself.

NOTATION:
Let $X = \{1, 2, \ldots, n\}$ and $\alpha : X \to X$ be a permutation. It is convenient to describe this function in the following way:

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{pmatrix}.$$

EXAMPLE:

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$$

CONCLUSION:
For a permutation we can use two different notations. For example, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$ and 24513 are the same permutations.

DEFINITION:
Let $X = \{1, 2, \dots, n\}$ and $\alpha : X \to X$ be a permutation. Let $i_1, i_2, \dots, i_r$ be distinct numbers from $\{1, 2, \dots, n\}$. If

$$\alpha(i_1) = i_2, \quad \alpha(i_2) = i_3, \ \dots, \ \alpha(i_{r-1}) = i_r, \quad \alpha(i_r) = i_1,$$

and $\alpha(i_\nu) = i_\nu$ for other numbers from $\{1, 2, \dots, n\}$, then α is called an r-cycle.

NOTATION:
An r-cycle is denoted by $(i_1 \ i_2 \dots i_r)$.

EXAMPLE:

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} = (1) \quad 1 - \text{cycle}$$

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = (1) \quad 1 - \text{cycle}$$

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (12) \quad 2 - \text{cycle}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13) \quad 2 - \text{cycle}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123) \quad 3 - \text{cycle}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = (1423) \quad 4 - \text{cycle}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = (13425) \quad 5 - \text{cycle}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix} = (125) \quad 3 - \text{cycle}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \quad \text{is not a cycle}$$

REMARK:
We can use different notations for the same cycles. For example,

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1) = (2) = (3), \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123) = (231) = (312).$$

WARNING:
Do not confuse notations of a permutation and a cycle. For example,

$$(123) \neq 123.$$

Instead, $(123) = 231$ and $123 = (1)$.

Composition (Product) Of Permutations

Let
$$\alpha=\begin{pmatrix}1 & 2 & \dots & n\\ \alpha(1) & \alpha(2) & \dots & \alpha(n)\end{pmatrix} \quad \text{and} \quad \beta=\begin{pmatrix}1 & 2 & \dots & n\\ \beta(1) & \beta(2) & \dots & \beta(n)\end{pmatrix}.$$
Then
$$\alpha\circ\beta=\begin{pmatrix}1 & 2 & \dots & n\\ \alpha(\beta(1)) & \alpha(\beta(2)) & \dots & \alpha(\beta(n))\end{pmatrix},$$
$$\beta\circ\alpha=\begin{pmatrix}1 & 2 & \dots & n\\ \beta(\alpha(1)) & \beta(\alpha(2)) & \dots & \beta(\alpha(n))\end{pmatrix}.$$

WARNING:

In general, $\alpha\circ\beta\neq\beta\circ\alpha$.

EXAMPLE:

Let $\alpha=\begin{pmatrix}1&2&3&4&5\\5&1&2&4&3\end{pmatrix}$, $\beta=\begin{pmatrix}1&2&3&4&5\\4&2&5&1&3\end{pmatrix}$. We have:
$$\alpha\circ\beta=\begin{pmatrix}1&2&3&4&5\\5&1&2&4&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\4&2&5&1&3\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\4&1&3&5&2\end{pmatrix},$$
$$\beta\circ\alpha=\begin{pmatrix}1&2&3&4&5\\4&2&5&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\5&1&2&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\3&4&2&1&5\end{pmatrix}.$$

REMARK:

It is convenient to represent a permutation as the product of circles.

EXAMPLE:
$$\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&2&6&9&5&7&1&8&4\end{pmatrix}=(1367)(49)(2)(5)(8)=(1367)(49)$$

REMARK:

One can find a composition of permutations using circles.

EXAMPLE:

1. Let $\alpha=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(123)$, $\beta=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(12)(3)=(12)$. We have:
$$\alpha\circ\beta=(123)(12)=(13)(2)=(13)=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},$$
$$\beta\circ\alpha=(12)(123)=(1)(23)=(23)=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}.$$

2. Let

$$\alpha=\begin{pmatrix}1&2&3&4&5\\5&1&2&4&3\end{pmatrix}=(1532)(4)=(1532),$$

$$\beta=\begin{pmatrix}1&2&3&4&5\\4&2&5&1&3\end{pmatrix}=(14)(2)(35)=(14)(35).$$

We have:

$$\alpha\circ\beta=(1532)(14)(35)=(1452)(3)=(1452)=\begin{pmatrix}1&2&3&4&5\\4&1&3&5&2\end{pmatrix},$$

$$\beta\circ\alpha=(14)(35)(1532)=(1324)(5)=(1324)=\begin{pmatrix}1&2&3&4&5\\3&4&2&1&5\end{pmatrix}.$$

THEOREM:
The inverse of the cycle $\alpha=(i_1i_2\ldots i_r)$ is the cycle $\alpha^{-1}=(i_ri_{r-1}\ldots i_1)$.

EXAMPLE:
Let $\alpha=\begin{pmatrix}1&2&3&4&5&6&7\\5&4&6&1&7&3&2\end{pmatrix}=(15724)(36)$. Find α^{-1}. We have:

$$\alpha^{-1}=(42751)(63)$$

In fact,

$$\alpha\circ\alpha^{-1}=(15724)(36)(42751)(63)=(1)$$

and

$$\alpha^{-1}\circ\alpha=(42751)(63)(15724)(36)=(1).$$

THEOREM:
Every permutation α is either a cycle or a product of disjoint (with no common elements) cycles.

Examples

1. Determine which permutations are equal:

(a) $(12)\neq 12$

(b) $(1)=12$

(c) $(1)(2)=(1)$

(d) $(12)(34)\neq(1234)$

(e) $(12)(34)=(123)(234)$

(f) $(12)(34)\neq(123)(234)(341)$

(g) $(124)(53)=(53)(124)$

(h) $(124)(53)=(124)(35)$

(i) $(124)(53)\neq(142)(53)$

(j) $(12345)\neq 12345$

(k) $(12345)=23451$

(l) $(23451)=23451$

2. Factor the following permutations into the product of cycles:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 5 & 4 & 6 & 7 & 8 \end{pmatrix} = (4\ 5)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 3 & 10 & 4 & 11 & 12 & 6 & 9 & 1 & 2 & 8 & 7 \end{pmatrix} = (1\ 5\ 11\ 8\ 9)(2\ 3\ 10)(6\ 12\ 7)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 2 & 12 & 7 & 9 & 14 & 8 & 4 & 5 & 3 & 6 & 10 & 11 & 13 & 15 \end{pmatrix} = (3\ 12\ 10)(4\ 7\ 8)(5\ 9)(6\ 14\ 13\ 11)$$

3. Find the following products:

$$(12)(34)(56)(1234) = (24)(56)$$
$$(12)(23)(34)(45) = (12345)$$
$$(12)(34)(56) = (12)(34)(56)$$
$$(123)(234)(345) = (12)(45)$$

4. Let $\alpha = (135)(24)$, $\beta = (124)(35)$. We have:

(a) $\alpha\beta = (143)$

(b) $\beta\alpha = (152)$

(c) $\beta^{-1} = (421)(53)$

(d) $\alpha^{2004} = (1)$

11. GROUPS

DEFINITION:

An operation on a set G is a function $*: G \times G \to G$.

DEFINITION:

A group is a set G which is equipped with an operation $*$ and a special element $e \in G$, called the identity, such that

(i) the associative law holds: for every $x, y, z \in G$,

$$x * (y * z) = (x * y) * z;$$

(ii) $e * x = x = x * e$ for all $x \in G$;

(iii) for every $x \in G$, there is $x' \in G$ with $x * x' = e = x' * x$.

EXAMPLE:

Set	Operation "+"	Operation "$*$"	Additional Condition
$\mathbb{N}$	no	no	—
$\mathbb{Z}$	yes	no	—
$\mathbb{Q}$	yes	no	"$*$" for $\mathbb{Q} \setminus \{0\}$
$\mathbb{R}$	yes	no	"$*$" for $\mathbb{R} \setminus \{0\}$
$\mathbb{R} \setminus \mathbb{Q}$	no	no	—

EXAMPLE:

Set	Operation "+"	Operation "$*$"
$Z_{>0}$	no	no
$Z_{\geq 0}$	no	no
$Q_{>0}$	no	yes
$Q_{\geq 0}$	no	no
$R_{>0}$	no	yes
$R_{\geq 0}$	no	no

EXAMPLE:

Set	Operation "+"	Operation "*"
$\{2n : n \in \mathbb{Z}\}$	yes	no
$\{2n+1 : n \in \mathbb{Z}\}$	no	no
$\{3n : n \in \mathbb{Z}\}$	yes	no
$\{kn : n \in \mathbb{Z}\}$, where $k \in \mathbb{N}$ is some fixed number	yes	no
$\{a^n : n \in \mathbb{Z}\}$, where $a \in \mathbb{R}, a \neq 0, \pm 1$, is some fixed number	no	yes
$\left\{\frac{p}{2^n} : p \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}\right\}$	yes	no

EXAMPLE:

Set	Operation
$\mathbb{R}_{>0}$	$a * b = a^2 b^2$ no
$\mathbb{R}_{>0}$	$a * b = a^b$ no